Trellix

We bring security to life.

March 17, 2023

Submitted via email to cyberframework@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 request for comments on '*NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*'

Trellix welcomes the opportunity to provide input to the NIST Cybersecurity Framework (CSF) 2.0 Concept Paper. 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 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 may be missing and what additions CSF may need.
- 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.
- 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, services and even product development risk evaluations but it is not optimal.
- 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 and use of it upon completion.
- Every organization develops software and thus the CSF should incorporate how an organization should be approaching secure software development and intellectual property protections, not necessarily for

commercial software, but for internal corporate needs. Additional considerations of how to tailor the Framework for project evaluation vs enterprise evaluation are needed. It may be that a Product Lifecycle Support Framework may need to be considered.

- 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 restrict adding new top level functions except where absolutely necessary, such as the proposed Govern function.
- 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.

Concept Paper Comments Requested:

1. CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications

1.1. Change the CSF's title and text to reflect its intended use by all organizations

Trellix Response:

We agree with this suggestion and believe this is in the best interest of the community and the CSF going forward. When we were initially developing the CSF, it was immediately apparent the CSF was being developed in a manner applicable to all organizations, large and small. However, the Executive Order 13636, issued by the President Obama on February 12, 2013, was titled "*Improving Critical Infrastructure Cybersecurity*". As a result, the initial CSF was titled "Framework for *Improving Critical Infrastructure Cybersecurity*". Many of the initial participants believed the title sent the wrong message to those that may potentially use and benefit from it.

1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size

Trellix Response:

While we too believe the CSF should be usable by all types of organizations, regardless of sector, type, or size, it is important to note this has generally been the case from the very initial version. Version 1.0 of the CSF states: "*The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today."*

During the process of CSF 2.0 development, if there are specific items that seem to run counter to the applicability of the Framework to a specific type of organization, we should make every effort to correct those.

Additionally, the intent indicated in 1.2 lists many U.S. related governmental uses/impacts. While accurate, it should be noted we should also look to assure the CSF is not targeted to any specific government. The CSF is addressing a global problem by focusing on cyber risk management. It is

important we assure the CSF continues to provide value not only based on sector, type, or size of an organization, but also the organization's global / national location.

1.3. Increase international collaboration and engagement

Trellix Response:

Trellix staff have long been active in international engagement with the governments of other countries in extoling the virtues of the CSF. As mentioned earlier, cybersecurity is a global problem and does not stop or start at an individual country's border. We applaud the actions NIST has taken in the past to align the world's organizations around a flexible way to address the principles and value of cyber risk management. We too will assist where we can, to continue to further encourage that global alignment.

2. CSF 2.0 will remain a framework, providing context and connections to existing standards and resources

2.1. Retain CSF's current level of detail

Trellix Response:

One of the more important factors in the adoption and value of the Framework is that organizations can pick up the CSF and use the informative references to start mapping what they are already doing. The Framework does not require wholesale changes to how an organization manages cyber risk. We are pleased NIST will be continuing to utilize that approach in CSF 2.0.

2.2. Relate the CSF clearly to other NIST frameworks

Trellix Response:

The Cybersecurity Framework has touched a lot of areas in its going-on ten year history. Section 2.2 in the 2.0 Concept paper discusses the need to relate the CSF clearly to other frameworks. In reality, we may want to ask the reverse question, "how do we clearly relate the other frameworks to the CSF". The Risk Management Framework, the Privacy Framework, the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity, and the Secure Software Development Framework will each remain separate frameworks and we agree with that. We cannot put all these valuable documents into a pot, stir thoroughly and come out with the "One Framework to Rule Them All".

Beside the specified NIST documents, there are other evolving and emerging areas needing to be properly addressed. IoT, OT, Product Lifecycle, Cloud, Zero Trust, AI, and more will be discussed and documented over the near future that are just as important to be clearly related in some fashion to the risk management aspects of the CSF.

We believe with the mix of topics and NIST related frameworks trying to be addressed in CSF 2.0, it is time to step back and consider an overall architectural approach to adding/linking other frameworks to CSF. It may be the CSF could be the "Core" with a family of directly related risk management frameworks more based on a specific technology of functional type. For example, there could be a more in-depth Product Lifecycle Framework incorporating the SSDF. Not all companies sell software. But for those that do, a Product Lifecycle Framework could be useful. How does that fit into the CSF family of risk management frameworks? It is obvious the CSF is the overarching risk management framework which other appropriate frameworks could be directly related or bridged to. As such, there needs to be discussions on how best to address emerging areas closely related.

2.3. Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core &

2.4. Use updatable, online Informative References

Trellix Response:

It is hard to answer the 2.3 and 2.4 individually. Let's be clear, the intent to put reference data online, where it could be much more dynamic and updatable, is a valuable tool for the community. While we understand the existing specific purposes of these two tools, we question the need for both as separate and distinct. Both of these capabilities could be enhanced by rethinking their highly focused uses. It appears that today, the two tools are there for how NIST manages documents and not how the community uses them.

The CPRT capabilities are great for selecting supported NIST documents, withdrawn, draft or final, and then searching for exact phrases within the selected document. It provides the ability to export the document or results in JSON or MS Excel formats. It does provide additional information as is the case with the Privacy Framework. See Shading Key for specifics. The CPRT depicts just what is in the published document. For example, the Privacy Framework did not include informative references in the released PDF document. It was intended these would be made available online so they could be updated and enhanced. Using the CPRT, there are no informative references made directly available.

The OLIR contains the "*Reference Data—Informative References and Derived Relationship Mappings (DRMs)"* and a search capability , a means for generating DRMs for specific documents and templates for submitting them to NIST. Useful but...

We have found having a set of informative references directly in the document is valuable to those actively reading and using it. During the Privacy Framework development, it was decided to NOT have a set of base level informative references included in the Privacy Framework 1.0. We have heard multiple times this makes it a harder to use and highly dependent on the OLIR. **Note:** *people have to learn how to use the CPRT and the OLIR in order to get what the intended purpose of these tools were meant to address*. Finding a base set or any specific set of standards and best practice mappings is now an adventure in clicking. There just seems to be something missing.

In keeping with the perspective of not identifying a real problem without providing a possible solution, we have an idea for NIST to consider.

IDEA: In many cases, organizations have based their cyber risk management on a specific set of international standards or industry best practices. Consider allowing CPRT users to select a set of standards or industry best practices and then provide a means for the user to generate a copy of the CSF 2.0 (or maybe another NIST framework document, such as the Privacy Framework) with the full text and the Informative References section of the Framework Core filled in with the selected mapped references. Allow it to print a PDF version, in addition to the XLSX and JSON formats. This would allow organisations to distribute a copy internally to their cyber risk management stakeholders, as was initially available in the 1.0 and 1.1 version of the CSF. The generated copy could be marked as generated by the CPRT. This would allow all the text and the Framework Core to be together in a highly convenient version for actual local needs and use. A new version could always be generated whenever a new or updated applicable standard or best practice document was added to the online references tool.

2.5. Use Informative References to provide more guidance to implement the CSF

Trellix Response:

As discussed in the comment to section 2.3 above, it is important there is a user focused tool that allows users to take advantage of the new sets of Informative References which NIST is encouraging industry to produce. We should be able to produce a generated version of the CSF in various formats (including PDF), with all the specific standards and best practices the user selects. We need to make the online CPRT and OLIR useful from a user perspective.

Updating individual informative references online

Currently supplying corrections to Informative References seems to be a "all or nothing" kind of approach being taken by NIST. While for the most part this makes sense, having the capability to map specific references to specific subcategories is also needed. For example, the RS.AN-5 informative references have little to do with the globally recognized coordinated vulnerability disclosure process this subcategory is addressing. The informative references for RS.AN-5 need to be corrected to reflect the internationally recognized ISO/IEC 29147 and ISO/IEC 30111 standards. How can we update specific or individual sets of Informative References instead of having a direct massive mapping to a specific document? While this is a single example, it is representative of an update capability needed for NIST documents with online references. Spot correction capabilities are needed. This specific update has been requested by us in the past. If there is a means to do this type of targeted reference update, it is not clear to us.

2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices

Trellix Response:

There is a need to try to deal with some of the harder new CSF topic areas planned for 2.0. Using Informative References to address specific cyber risk domain issues allows the Framework to remain consistent with its initial goals of being a framework. Supply Chain security is a perfect example. It is not necessary to incorporate all supply chain issues into the Framework directly. Address it from a high level framework perspective and use new categories and/or subcategories with Informative references pointing the valuable work that has been done throughout the last few years. The CSF will not get it right by itself. It needs to leverage the existing body of work in this area. Informative References allow for the CSF to take advantage of that great work.

We are pleased to see NIST's continued focus on remaining technology-neutral while assuring the CSF's broad outcomes can continue to be used regardless of the specific technology or services employed.

One area that is starting to get a bit frustrating is the overuse of specific terms with the CSF environment. The use of the term 'profiles' is highly confusing. Often they are talked about as generic but expected to be used for highly specific purposes. There are many different uses of the term profiles that were heard and discussed at the in-person CSF 2.0 event in February 2023.

- Enterprise Profiles
  - Target Profile
  - Current Profile
- Industry Profiles
- Sector specific Profiles

- Product Profiles
- Service Profiles
- Sample Profiles
- Example Profiles
- Technology specific Profiles
- High-level Generic Profiles
- Threat-informed Profiles
- ...

And the format for profiles varies by those that create them such as the "Framework Payroll Profile - IRS Security Summit". The Examples of Framework Profiles page is an example of the lack of proper focus when discussing profiles. Are they just simple checklists that one sector or technology should be evaluating themselves against? In our minds a checklist is not a CSF profile.

This is a problem that needs discussion as it was apparent that more than a few people attending the in-person workshop were calling everything a profile. Profiles have specific meanings according to the CSF 1.0 and 1.1 and specific needed information. Maybe it is time to extend the "Core" architectural definition so that there is the concept of overlays that extend the core. The use of the term profile is not consistently understood or applied. This can be confusing to those that are trying to apply the CSF.

3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

Trellix Response:

Trellix was one of the 500 voices asking for additional materials to support the adoption and integration of additional guidance into the set of supporting materials. In some cases, we feel the CSF itself needs to have additional verbiage as to the use of the CSF. Too many people want to use the CSF as an implementation checklist. This approach actually diminishes the value of the Framework. We consider the Framework, just that, a framework that should be molded to the organization's needs for evaluating their cyber risk management needs. This is how we have seen it be the most effective. More focus on describing potential modifications as to how to adapt the Framework would be beneficial. Tiers is one area where customization can easily add a great deal of value.

3.1. Add implementation examples for CSF Subcategories

Trellix Response:

We too believe notional examples would benefit those trying to understand the CSF but are a bit confused as to what is meant by a small number. While we understand that including them to the extent the SSDF did could be incorrectly interpreted as a baseline requirement, with the proper contextual disclaimers that concern could be addressed. There is also a statement:

> *The examples may also help to address the evolving nature of cybersecurity technologies and techniques by highlighting possible differences in implementations for platforms such as IT, IoT, OT, and cloud computing.*

We caution about putting this type of information in the CSF directly. Information contained in the CSF should be viewed as the Core of a family of frameworks, with the Core focus on the organizational enterprise risk management concerns.

In-depth implementation examples should be relegated to an external supporting document external to the base CSF 2.0 specification. In this manner, specific guidance can be developed for sector or technology-specific areas without compromising the intent and value of the CSF.

While the model used by the SSDF was interesting and useful, like informative references, the examples could become stale over time as better or more different examples emerge. Keeping this external to the CSF allows supporting guidance documents to be updated on a much timelier basis without the community impact of republishing the entire CSF.

3.2. Develop a CSF Profile template

Trellix Response:

This is a hot button topic from our perspective. The use of the term Profile is overused and little understood. Is the profile just a subset of the CSF with all the same elements of the Core CSF? It is used in a variety of ways to describe add-ons too, subsets of, and overlays for, the CSF. The term profile needs to be truly clarified because it is one of the more confusing aspects of the Framework when not talking about the Current or Target Profiles.

Some of the "profiles" listed on the NIST website that have be donated to the effort are not even in a format similar to the Framework Core. So, if syntax and format are not important, what is a profile?

Maybe what NIST needs to do it to define profiles as

> *Framework Profiles are a way in which organizations implement the CSF by aligning the CSF's Functions, Categories, Subcategories and Informative References with the mission requirements, risk tolerance, and resources of an organization. The format of profiles must follow the CSF structure if they are to be used external to the organization that created it, such as a sector-specific or community example profile.*

The CSF Core is the Profile Template. Maybe more wording needs to go into why an organization would want to create a modified Profile than to worry about spending cycles developing tons of example "profiles".

3.3. Improve the CSF website to highlight implementation resources

Trellix Response:

As an organization that has contributed both a success story and the DDOS and Botnet profiles to NIST, we agree there is a need to improve the usability of the NIST CSF website. The call to actions were appreciated as there is a vast set of knowledge and experience, and potentially materials, that could be crowdsourced for the benefit of the global risk management community. More should be done to incentivize that community to contribute.

4. CSF 2.0 will emphasize the importance of cybersecurity governance

Trellix Response:

The addition of the GOVERN Function is both a plus and minus. Minus because everyone that is familiar with the Framework is able to rattle off the Identify, Protect, Detect, Respond & Recover. That includes C-suite and Board members. Now we will have to teach them that GOVERN needs to be added. For executive management, that will probably not be too hard, but to those in the trenches it might take a bit longer.

We believe the Privacy Framework added the perspective of how to stand up a Privacy Office for organizations that did not have one. It also had existing Privacy Offices reviewing their processes and procedures to assure they were GOVERNing correctly according to the Privacy Framework. The CSF did not have this initially and in retrospect, needed to. With CSF 2.0, we have the opportunity provide a perspective for corporate Risk Offices that reflects what the Privacy Framework provided.

4.1. Add a new Govern Function

Trellix Response:

Yes and very much appreciated.

4.2. Improve discussion of relationship to risk management

Trellix Response:

Yes, this focus will bring clarity to cybersecurity risk management as it applies to the use of the CSF. This was a core intent when we initially were discussing the development of the Framework in 2013.

5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)

Trellix Response:

While we agree that supply chain affects all organizations, not all organizations create commercial software for sale. There are areas of cybersecurity supply chain that needs to be addressed in the framework and other areas that are out of scope directly in the CSF. The focus of the improvements for C-SCRM in the CSF should be reflecting those items that the majority of organizations need to consider in their risk management decisions and operations. This is a very large topic area if all aspects of the C-SCRM were to be included. NIST and the CSF should focus and not become the kitchen-sink of C-SCRM concerns. There has been a great deal of detailed and useful work in this area and the CSF should leverage this great work via the use of Informative References.

5.1. Expand coverage of supply chain

Trellix Response:

We agree with NIST that additional outcomes should be included to support C-SCRM specific considerations. We fully endorse the creation of subcategories, and even categories as needed.

We do not believe it is necessary to create an entirely new supply chain top-level Function. C-SCRM would be better integrated within the existing CSF subcategories, with the potential for new subcategories as required. With the development and agreement of a new GOVERN Function, C-SCRM has another appropriate place to be addressed.

And ...

Since the SSDF is mentioned here, we believe there should be serious considerations given to the development of a "Software Product Lifecycle Framework" that would examine and recommend not just the SSDF perspective but look at the complete secure product lifecycle process. This could become a real model for IoT, consumer and commercial software products lifecycle support. Today the CSF can be "contorted" to be used in this way, but it is far from complete. We believe NIST would seriously advance the goals of the Cyber EO (EO 14028) by developing this sort of document, of which the SSDF would be a part. Related areas of C-SCRM could then be incorporated in detail in that document.

6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment

Trellix Response:

As an organization that was one of the first to explore the value of Tiers in measuring the CSF's effectiveness, we wholeheartedly agree. At the in-person working sessions someone said they saw no value in and did not use the Tiers. We wonder how they use the Framework at all.

More information is needed to explain how the Framework components all fit together and can be used to measure the progress of the organization's cyber risk management objectives.

6.1. Clarify how leveraging the CSF can support the measurement and assessment of cybersecurity programs

Trellix Response:

We believe the description of this section is exactly what is needed to be made clearer in CSF 2.0. It must be understood by reading the Framework document that when we are talking about measuring we are talking about measuring the organization's journey toward improving their cyber risk management goals utilizing the CSF.

6.2. Provide examples of measurement and assessment using the CSF

Trellix Response:

We believe that much of the discussion on measurement and the CSF has resulted from many people and communities talking past each other. Measurements and metrics are in the eye of the beholder. For example, there are control level metrics, process measured metrics, results and outcome related metrics, periodic or trending metrics, ... So, what is it that we are discussing when we talk about measurements and metrics in relation to the CSF?

We believe the metrics we are documenting in the CSF should be focused on the status, process improvements and trending measurements of the enterprise's cyber risk management journey. They should not be on measuring the results of individual and specific controls the CSF may reference. It should be instead focused on the progress made by the organization on each of the individual subcategories they are examining and assessing themselves by. Measurement of the current status (Current Profile) against what the organization's level of acceptable risk (Target Profile), using Tiers to produce actionable results, is what we should be describing. These sorts of results have shown to be a highly informative means for determining where an organization stands at a point in time and how they have improved (or not) over past assessments.

Trying to establish a generic way to measure "cybersecurity" is fruitless and impossible. Trying to measure a journey based on the CSF is not only doable today but highly informative for organization needing to consider where real impactful cyber risk improvements need to be made. We have successfully seen the CSF point out ,not only gaps that need focus, but over-spends when the assessed level exceeds the protections needed for that subcategory. That was a great message for the corporate accountants. Cyber dollars could be transferred to other needed areas without asking for more money in the budget.

The CSF Measurement discussions should focus on how that type of measurement can add value to the organization. We cannot and do not need to get to a single number as many have suggested. Measure the progress or lack thereof is what the CSF should be focused on.

6.3. Update the NIST Performance Measurement Guide for Information Security

Trellix Response:

Informational so no response needed.

6.4. Provide additional guidance on Framework Implementation Tiers

Trellix Response:

We cringe to this day when the CSF is mentioned in the same a breath as a maturity model. It is not. It is an organizational risk reduction progress model. That is very different from a maturity model where organizations need to achieve a standardized industry-wide indicator with a single top level achievement everyone is striving for. The CSF is measuring the risk improvement journey the organization is on. We do not measure one item but a set of items that show where we stand against the organization's level of acceptable risk. Every organization's set of decisions will be different, even when they are in the same sectors. No one is going to say (seriously) "we are an Adaptive Tier 4 level CSF organization".

Tiers have always been understood to be focused on goals and objectives. While it could be made clearer in the CSF, that is the way we have viewed then in the past. Improvements need to occur in all areas and external participation is vital in today's threat landscape. We modified Tier definitions to focus on a People, Process, Technology and Ecosystem approach while keeping the numerical meanings. We would be happy have an in-depth discussion of how that approach has proven valuable for us in how we see the Framework and how we measure our success.

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 a great deal of new and emerging areas of cyber risk into the CSF, 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 concept paper. 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 associated cyber risk management capabilities.