Initial Summary Analysis of Responses to the Request for Information (RFI) Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

National Institute of Standards and Technology (NIST)

June 3, 2022

Introduction

On February 22, 2022, NIST issued a public Request for Information (RFI), "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management." The RFI sought information on the use of the NIST Cybersecurity Framework as well as recommendations to improve the effectiveness of the Framework and its alignment with other cybersecurity resources. The RFI also sought suggestions to inform other cybersecurity efforts at NIST, especially related to supply chain cybersecurity risks. When the RFI was issued, Commerce Deputy Secretary Don Graves stated: "Every organization needs to manage cybersecurity risk as a part of doing business, whether it is in industry, government or academia...It is critical to their resilience and to our nation's economic security. There are many tools available to help, and the CSF is one of the leading frameworks for private sector cybersecurity maintenance. We want private and public sector organizations to help make it even more useful and widely used, including by small companies."

This document represents an initial, high-level summary of the RFI responses. NIST received more than 130 RFI responses, including many comments submitted jointly by multiple organizations or associations representing numerous organizations. The responses can be found on the NIST CSF website.

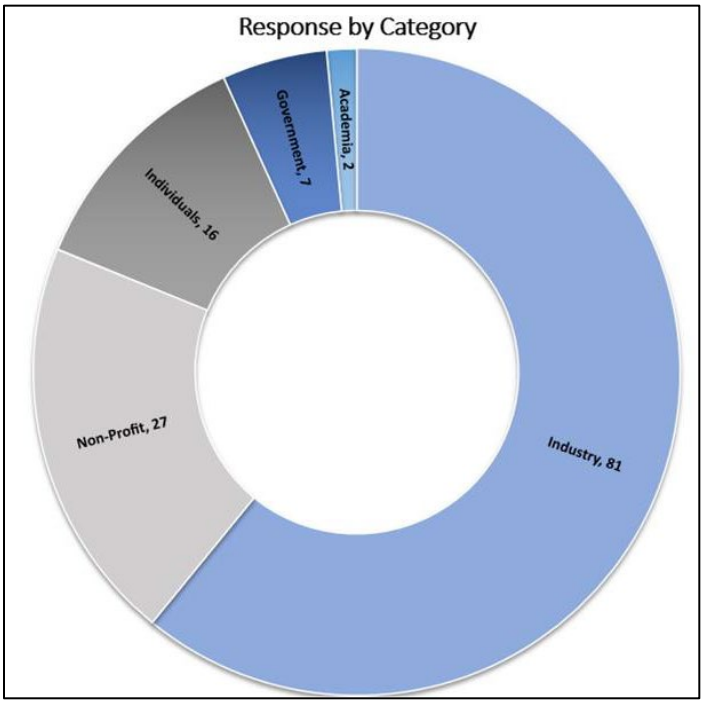

Figure 1 RFI Responses Received by Category

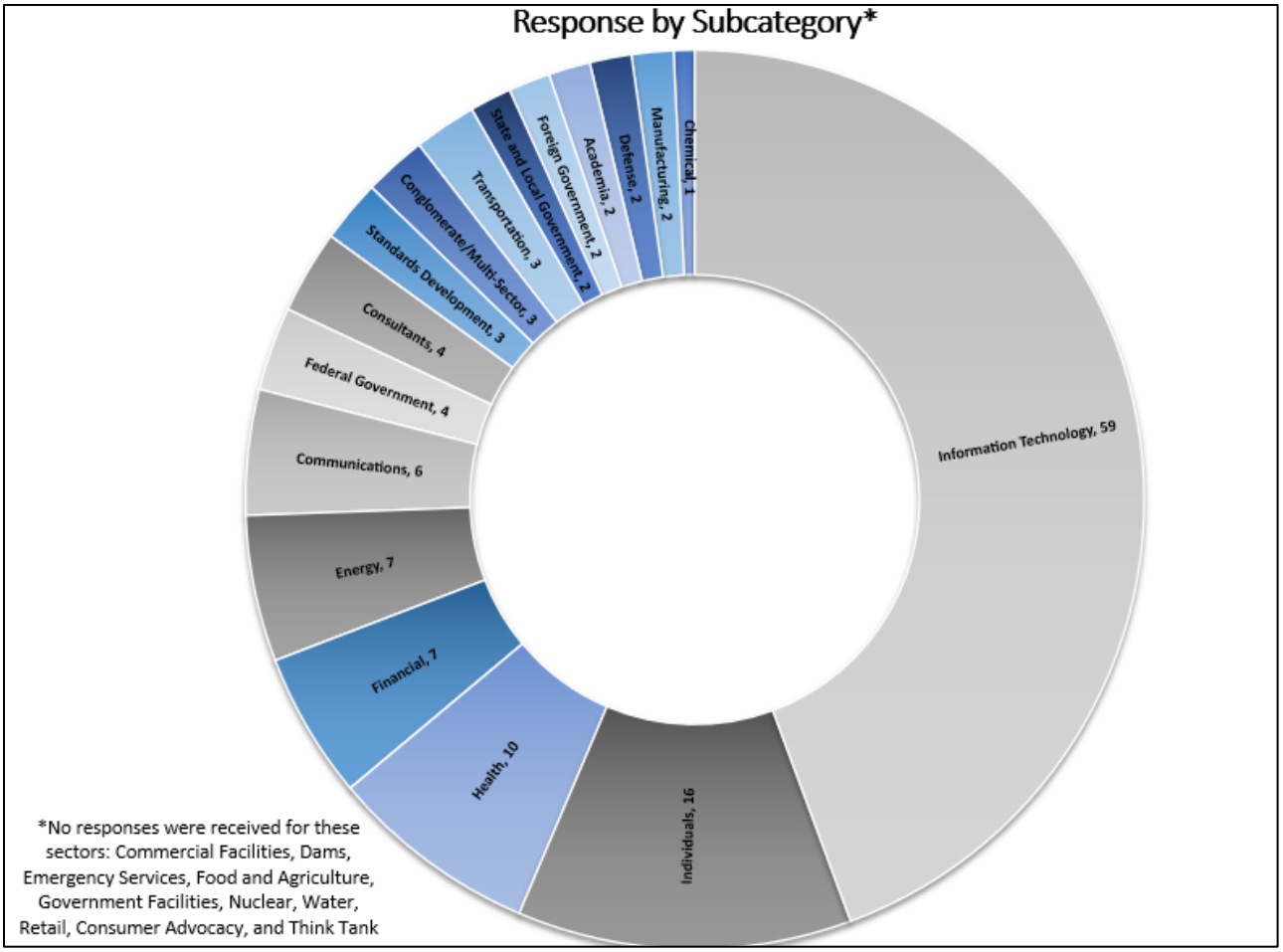

Figure 2 RFI Responses Received by Subcategory

The NIST Framework for Improving Critical Infrastructure Cybersecurity (also called Cybersecurity Framework, Framework, or CSF) was released in February 2014 after extensive public engagement and collaboration. The Framework serves as a prominent resource to manage cybersecurity risks holistically across an organization. It has been downloaded over 1.7 million times and is used by organizations of varying sectors, sizes, and locations. It has been adopted internationally, with the English version complemented by nine translations.

The CSF was intended to be a living document that is refined, improved, and evolves over time to keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice. NIST updated the Framework in April 2018 with CSF 1.1. Based on the RFI responses, and in order to keep pace with the ever-evolving cybersecurity landscape and to help organizations more easily and effectively manage cybersecurity risk, NIST is planning a new update to the Framework.

The RFI also sought information on the challenges organizations are facing from a technology supply chain perspective to inform the NIST-led public-private partnership, the National Initiative for Improving Cybersecurity in Supply Chains (NIICS). NIST requested information about needed supply chain tools and guidance, as well as how NIICS might be aligned and integrated with the CSF.

This summary analysis will serve as a starting point for scoping the update to the NIST Cybersecurity Framework, as well as scoping NIICS.

NIST intends to continue to rely on and seek stakeholder feedback throughout the process to update the Framework. This will include public webinars and workshops, as well as feedback on at least one Framework draft. Stakeholders are invited to evaluate the themes identified by NIST, determine if these themes appropriately reflect comments received through the RFI, and begin identifying specific ways in which NIST can address these themes to guide the Framework update process.

1. Methodology

NIST analyzed each RFI response to:

- determine respondent information, including sector, size, and organization type;
- identify specific recommendations for the Framework update, including which sections of the Framework or other topics are addressed by the response; and
- identify key points, commonalities, and recurring concepts among the responses – which are reflected in the themes.

2. Themes from RFI Responses

Based on a review of the responses, NIST identified commonalities and key areas of agreement and differences. These are identified as seven themes and 25 subthemes. Of these, six themes and 20 subthemes apply to the Cybersecurity Framework. One additional theme and five subthemes apply to NIICS, recognizing that there may be some overlap with the Framework.

Excerpts from various RFI responses are included to illustrate themes and subthemes. These excerpts are representative only; they are not intended to be an exhaustive review of all the responses received on a particular theme.

Theme 1: Focus on maintaining and building on the key attributes of the CSF with the update.

RFI respondents highlighted numerous ways in which the Cybersecurity Framework has been effective in helping organizations understand and manage cybersecurity risks. Key desired attributes of the CSF – including its flexible, simple, easy-to-use, and voluntary nature – have been beneficial for implementation by organizations of varying sizes and sectors. In addition, the Framework has been effective in enhancing communication within and across organizations.

Most commenters agreed that NIST should seek to maintain these key attributes with the update. In addition, because of the attributes, several commenters requested avoiding changes to the fundamental structure of the CSF or making significant changes to the CSF. Nevertheless, comments included substantive recommendations for improvement among the more than 4,000 total recommendations across the comments. The following subthemes highlight respondents' recommendations to maintain the beneficial attributes of the CSF 1.1 while building upon that foundation and enhancing CSF's usefulness in CSF 2.0.

Subthemes:

1.1 The CSF is widely used and effective in helping organizations understand and manage cybersecurity risks.

1.2 The flexible and voluntary nature of the CSF has been beneficial for implementation by organizations of varying sizes and capabilities.

1.3 Ensure the CSF is simple and easy to use.

1.4 Keep the CSF effective in enhancing communication with non-IT and security stakeholders, including the C-suite.

1.5 Maintain backwards compatibility.

Theme 2: Align the CSF with existing efforts by NIST and others.

RFI comments highlighted the need to retain and improve alignment of the CSF along with other NIST and non-NIST resources and models. The CSF was designed to provide a common organizing structure for standards, guidelines, and practices. Because it references globally-recognized standards for cybersecurity, the CSF supports coordination and communication within the U.S. and serves as a model for international cooperation on strengthening cybersecurity.

Since the release of CSF 1.1 in 2018, NIST has published new cybersecurity resources including an update to Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5), the NIST Privacy Framework, the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity Rev. 1 (SP 800-181), the NIST Secure Software Development Framework 1.1 (SP 800-218), Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286), the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Operational Technology (OT) Security (SP 800-82 Rev 3 draft). While CSF complements many existing resources

from NIST and from numerous other sources, comments expressed a need for NIST to improve and expand those alignments and also to provide additional guidance on how to use these various standards, methodologies, procedures, and processes together. In some cases, commenters expressed that the resources should be aligned, while others recognized a need for additional mappings between and among the resources.

Commenters also shared feedback about the role that governance of cybersecurity risk management can play in the CSF, especially as the CSF has historically been valued as a process that supports coordination of cybersecurity activities throughout the enterprise. However, feedback varied on how to address governance in the CSF.

Several additional elements of this theme align with activities described in the NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1. This roadmap described NIST's next steps with the CSF and identified areas for further development. Much progress has been made in these roadmap areas, including advances in privacy, supply chain, and international coordination. The subthemes below include recommendations regarding CSF alignment with NIST resources, engagement with other federal agencies, and continued (and increased) international collaboration.

Subthemes:

2.1 Align the CSF with recent NIST efforts reflected in a variety of resources.

2.2 Make it easier to understand how the CSF can be used with other cybersecurity guidance; provide more mappings with the NIST National Online Informative References Program (OLIR) and Informative References.

2.3 Address the important role of governance in cybersecurity risk management, although there are several different approaches for doing so.

2.4 Improve alignment between the CSF and NIST privacy resources.

2.5 Engage with other federal agencies to ensure effective use of the CSF for policy, legal, and regulatory purposes.

2.6 Increase international collaboration and engagement, including alignment with the ISO 27000 series.

Theme 3: Offer more guidance for implementing the CSF.

The CSF was designed to be technology- and vendor-neutral, and to apply across sectors. As such, the level of detail and specificity in the CSF reflects the scalability and flexibility necessary to meet the needs of a wide range of stakeholders – small and large organizations in various sectors. There were more than 500 references in the comments supporting the need for more guidance to support CSF implementation, and many users expressed a desire for greater detail in the CSF while maintaining a non-prescriptive approach. Identifying the proper balance between simplicity and detail in updates to the CSF is a key takeaway that will need further discussion.

Subthemes:

3.1 Offer more guidance on CSF implementation.

3.2 Provide specific guidance on developing CSF profiles.

Theme 4: Ensure the CSF remains technology neutral but allows it to be readily applied to different technology issues – including new advances and practices.

In establishing the CSF, Executive Order 13636 directed that "[t]o enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks." Commenters pointed to both the benefits and challenges of the CSF's technology-neutral and vendor-neutral design. Some noted that while technology has evolved since the initial creation of the framework, the CSF functions and outcomes continue to support organizations' risk management and cybersecurity program improvement. The benefits of a technology-neutral approach were broadly recognized, but multiple commenters said that changes may be necessary to ensure the CSF update clearly addresses cybersecurity for different types of systems – including IT, OT, IoT, and cloud computing. In addition, given the recent guidance developed under Executive Order 14028, commenters suggested that additional consideration be given in the CSF to software security. As with other themes, respondents called for a flexible approach that applies to all organizations using the CSF.

Subthemes:

4.1 Ensure the CSF remains technology neutral while providing guidance on how it is used to address cybersecurity risks in IT, OT, and IoT.

4.2 Consider the importance of software security, either as part of the CSF or in conjunction with the CSF.

4.3 Ensure the CSF remains technology neutral yet can be applied to specific and emerging topics such as cloud, hybrid work, and zero trust.

Theme 5: Emphasize the importance of measurement, metrics, and evaluation in using the CSF.

Numerous stakeholders indicated a need for additional CSF guidance and resources to support cybersecurity metrics and measurement. Many described an opportunity to improve measurement of cybersecurity risk management in the CSF update. Some comments called for more specific guidance regarding how to measure achievement of CSF outcomes. Others called for the CSF (or supporting materials) to include suggested metrics and examples. Further guidance for measuring the performance of an entity in establishing and improving a cybersecurity program was a key need expressed in the RFI responses. However, there were varying viewpoints around the value and use of the Tiers and whether the CSF should be expanded to include guidance on maturity models.

Subthemes:

5.1 Consider and highlight how the CSF is used as an assessment tool, including consider additional guidance on assessment (for self, suppliers, products, and services).

5.2 Provide a means to measure CSF implementation.

5.3 Expand on (or, in contrast, remove) Tiers and include (or do not include) guidance on maturity models.

Theme 6: Consider cybersecurity risks in supply chains in the CSF.

Responses broadly supported increased references to supply chain risk management in the updated CSF. Many commenters considered whether a new supply chain-specific framework is needed and recommended expanding and improving the CSF to address that need rather than create another model. The comments urged NIST to develop additional guidance and reference materials to help organizations address supply chain risks.

Subtheme:

6.1 Address supply chain risks, either in the CSF or separately.

Theme 7: Use the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to align practices and provide effective practices, guidance, and tools to bolster cybersecurity supply chain risk management.

Comments also provided input on cybersecurity challenges in supply chains to help NIST scope NIICS. Commenters broadly recognized the importance of cybersecurity supply chain risk management (C-SCRM), especially in light of recent security incidents. Many organizations, particularly small enterprises, recognize the importance of C-SCRM but are resource constrained, so having a single clearinghouse for guidance, templates, tools, and information sharing would be of great benefit.

Subthemes:

7.1 Align cybersecurity supply chain risk management practices, including federal activities and resources.

7.2 Offer more guidance on component inventories, such as software bill of materials and hardware bill of materials.

7.3 Engage on open-source software security issues.

7.4 Offer more guidance on supplier relationship management and contracts.

7.5 There are opportunities for NIICS to research, analyze, and develop tools and techniques for better managing cybersecurity risks in supply chains.

Theme 1: Focus on maintaining and building on the key attributes of the CSF with the update.

1.1 The CSF is widely used and effective in helping organizations understand and manage cybersecurity risks.

A large majority of respondents shared that they have found the Cybersecurity Framework to be a useful model for organizations seeking to identify, assess, address, and manage cybersecurity risk. They described many benefits that result from the use of the Framework in providing common language and systematic strategy for addressing cybersecurity risks. Many commenters shared that the Framework plays a key role in aggregating and communicating risk management insights to stakeholders at many levels.

RFI Response Examples

- "…the NIST CSF is an essential resource that supports cybersecurity governance and risk management activities. Our company relies broadly upon the CSF, and in particular, has made it the foundation of our enterprise cyber maturity assessment program."
- "Alignment of the NIST CSF to the five functions in the framework is a remarkably effective means to communicate at all levels (and technical competencies) of an organization…"
- "Broad swaths of the business community support the popular Cybersecurity Framework…"
- "NIST Cybersecurity Framework has become the de facto standard for many organizations all over the world, of all sizes, scopes, and complexities. Our client organizations find NIST Cybersecurity Framework Functions, Categories, and Subcategories extremely helpful for organizing, managing, aggregating, and reporting their cybersecurity program activities."
- "As NIST considers potential updates to the Framework itself, it should remember that the framework as it exists has been widely successful and should not seek to materially change the Framework Core."
- "The Cybersecurity Framework has been a tremendously successful tool for evaluating and managing cybersecurity risk by organizations large and small. Its success results from NIST's collaborative approach to development and implementation of the Framework, driven by technical expertise and bolstered by NIST's receptiveness to stakeholder input and recommendations."
- "The five functions of the CSF are applicable regardless of organization sector, size, or structure…The five functions provide structure through a common language to discuss cybersecurity capabilities, programs, and practices. The CSF is a tool that can be used to demonstrate and communicate progress or need for further actions in the five functions."
- "A major advantage of the CSF is that it provides a common language and systematic methodology for managing cybersecurity risk. …[commenter] consists of about 900 different operating companies. These companies are very diversified in their service offerings, geographic locations, and business models. The CSF fits very well for providing a common language to this diversified group of companies."

1.2 The flexible and voluntary nature of the CSF has been beneficial for implementation by organizations of varying sizes and capabilities.

An attribute of the CSF has been its flexibility, which allows implementation across organizations of varying sizes and types. Respondents recognized the benefits of that flexibility to address various cybersecurity risks, risk thresholds, and technologies, as well as implement other frameworks and legal responsibilities. The flexibility also allows the Framework to be used as a starting point for small-to-medium-sized organizations, while also being adaptable for larger organizations with existing risk management programs.

RFI Response Examples

- "The CSF is an effective tool to aid organizations' cybersecurity efforts and the flexible, voluntary nature of the framework has greatly helped in its adoption."
- "The Framework needs to continue to be as widely applicable and as flexible to use as possible."
- "In general, this is something that the NIST CSF has historically gotten right. We wish to note that [commenter] has frequently pointed to the NIST CSF as an example of government standards-setting done right because it is: a. Done in collaboration with industry b. Technology agnostic c. Voluntary d. Not 'one size fits all.'"
- "Continue to maintain the outcome-level nature of the NIST Cybersecurity so that it complements rather than competes with other national and international cybersecurity control and risk management frameworks, whether in the private or government sector."
- "Four drivers of the benefit the Framework creates stand out. First, because it is risk-based and flexible, it can be used by diverse organizations in any sector. Second, because it is widely used, it contains a lingua franca for communicating about cybersecurity risk management. Third, because it is written at an appropriate level, high enough to be universal but detailed enough to drive cybersecurity risk management, it is usable. Fourth, because organizations use it and provide their documents to NIST, the informative references lower the barrier while simultaneously amplifying the benefits to use."
- "The five functions provide helpful guidance to organizations that are establishing their cybersecurity risk management systems from scratch. At the same time, the flexible design of the functions enables organizations that have already established and been managing their own risk management systems to overlay the Framework Core to review and improve their existing risk management process."

1.3 Ensure the CSF is simple and easy to use.

Respondents pointed out that the CSF has provided a model for managing and communicating about cybersecurity. Comments recognized that an update may bring additions and complexity and urged NIST not to lose the current simple-to-use model. Some recommended the use of supplemental documents and resources for providing additional information rather than adding complications or extensive detail to the CSF itself.

RFI Response Examples

- "[Commenter] recommends that any updates that NIST makes to the CSF should continue to utilize the Framework's architectural design simplicity, be incremental in scope, and that NIST undertake specific initiatives to make sure that the CSF's use is sustainable. Keep it Simple. Incremental. Sustainable."
- "…[commenter] urges NIST to do everything in its power to do ensure that the Cybersecurity Framework remains the host helpful 21 pages in cybersecurity… [Commenter] understands that limiting the length of the document creates a significant challenge – but it is precisely NIST's ability to meet that challenge, to include only the most important concepts, language, and references, that create value."
- "Likewise, it is important for NIST to balance new additions with the understanding that organizations around the world have already previously adopted the CSF into their risk management practices, and therefore new additions should be calibrated to reflect the evolving landscape but also be principle-based to ensure that organizations are implementing sound practices without chasing multiple new risk management requirements. A continued focus on simplicity will help to achieve this and we encourage NIST to make updates to the CSF in a manner consistent with the current CSF so that it remains easily understood and adaptable."
- "While it is reasonable that the CSF is kept concise and high level for universal use, those new to the CSF may have some difficulty conceptualizing a concrete implementation. Given that the CSF is often the first document referenced regarding cybersecurity risk management in many organizations, supplemental information regarding implementation details could be added."
- "The five functions are of significant value to organizations who are relatively immature and new to cybersecurity as it provides a simple lens through which to understand the field and the areas in which they are likely to require investment."
- "To be more accessible and approachable, the framework understandably boils down complex ideas and cybersecurity constructs in to simple, short phrases...These are complex issues and require attention paid to specific controls in NIST SP 800-53 and the other references provided by NIST. Unfortunately these references are often overlooked by organizations."
- "It's simple to grasp and yet subtle to achieve."

1.4 Keep the CSF effective in enhancing communication with non-IT and security stakeholders, including the C-suite.

A key attribute of CSF 1.1 is the ability to use its outcomes and process for stakeholder engagement. The CSF is designed to support communication among technical and non-technical participants at all levels of the enterprise. As with the subthemes described above, respondents shared opportunities to improve those communications and urged NIST to ensure that any planned updates continue to support enterprise-wide collaboration.

RFI Response Examples

- "The NIST CSF provides industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to operations."
- "Due to the risk-based and business-operations approach of the CSF, where the NIST CSF has been implemented, it is much more easily grasped and used by non-IT and non-security executives. This drives more engagement, participation and interest in security than those frameworks which are more technically focused and controls based."
- "As before, the Framework should be as short as possible and not encyclopedic. The target audience for the Framework is the C-Suite and the Board of Directors, not the technical or engineering community, and it should be drafted appropriately. It should lay out specific requirements and objectives with as much specificity as possible."
- "Specifically, its usefulness derives from its ability to provide an approachable framework to organize cybersecurity activities, help facilitate communication regarding risk and how risk is considered within the organization, and prioritize opportunities aligned with objectives and requirements."
- "…to the extent the goal of the Framework was to provide a common language for organizations, it has certainly achieved that, proving useful for communicating about cyber risk both within and between organizations."
- "The functions selected in the framework contemplate the most important actions when thinking about Cybersecurity processes and allow a high-level perspective beyond specific activities facilitating the communication of strengths and weaknesses to senior management of the organization."
- "The most significant advantage of the framework is the five functions, and the simplicity and clarity that it allows in communication to non-cyber-security professionals including Boards of Directors."

1.5 Maintain backwards compatibility.

Many of the responses shared examples of how organizations have implemented the CSF including mappings, assessment methodologies, and communications processes. Many respondents made it clear that improvements are welcome but that an updated CSF must retain compatibility with previous versions.

RFI Response Examples

- "[Commenter] believes that the usability of the framework is a key item for organizations that wish to implement it. We caution NIST against any overall structural change to the existing framework that might decrease its usability or substantially undermine security investment rooted in the original framework."
- "Given the amount of cybersecurity activity currently underway, it may be prudent for NIST to consider waiting on a major update."
- "Our concern with modifying the CSF is that many organizations use [governance] risk & compliance tools (GRCs) and that these tools map to the CSF, therefore, any changes will break the mappings and will require substantial effort to remap which will affect numerous internal operations such as audits."
- "To minimize the impacts limiting usability and backward compatibility, we recommend NIST limit changes to the lowest levels [*context from previous paragraph of response references changes at the categories and subcategories level]* of the CSF as possible."
- "Backward compatibility would be most severely impacted by changes to the subcategories because that's where the mapping to other frameworks happens. Additions, just as you'd make to 800-53, should be low impact."
- "[Commenter] supports the evolution of the Framework to meet the changing landscape of cybersecurity risks…As the current Framework has already been widely adopted and tailored by entities across critical infrastructure sectors, the structure of the Framework Core should be preserved to the extent possible."
- "We believe that useability and backward compatibility are important, but the world and the practice have changed substantially. We would advise NIST to keep the structure the same, fill in the gaps that the community identifies, but keep constant those parts of the framework that can be kept constant."
- "Many organizations utilize the CSF on an ongoing or annual basis. Backward compatibility is crucial for organizations to measure progress. If backward compatibility is not possible, at the very least, an accounting of changes and a mapping between versions will be necessary."

Theme 2: Align the CSF with existing efforts by NIST and others.

2.1 Align the CSF with recent NIST efforts reflected in a variety of resources.

NIST conducts research, development, and outreach to advance and develop cybersecurity standards, guidelines, and practices to advance cybersecurity risks. Since the release of CSF 1.1 in 2018, NIST has released new cybersecurity resources that include an update to Security and Privacy Controls for Information Systems and Organization, the NIST Privacy Framework, the NICE Workforce Framework for Cybersecurity, the Secure Software Development Framework, IoT and OT cybersecurity guidance, and enterprise risk management guidance. Comments included broad requests to align the CSF with these other efforts. Alignment between these key resources, as well as identification of efficient ways to apply these multiple products, will help improve adoption and reduce cybersecurity risks.

RFI Response Examples

- "We recommend the continuation and timely update of linkage/mapping between NIST CSF and other cybersecurity framework. The linkages should allow NIST CSF to stay relevant in between version updates, as it maps to newer frameworks or frameworks refreshed to update our understanding of cybersecurity."
- "[Commenter] agrees with the RFI that NIST should actively work to harmonize the CSF with related NIST tools published since the release of CSF V1.1."
- "In general, the more integration and compatibility between CSF and key NIST products…. A critical factor is ensuring that the integration is not a one-way proposition. In other words, the CSF should provide overlap and mapping to these frameworks and vice versa."
- "NIST provides two major resources regarding risk management: the CSF and Risk Management Framework (RMF)… As each framework has its own scope and perspective, additional explanation on the relationship among related resources including the CSF and RMF, both in similarity and difference for a particular scope, typical use cases, etc. could be beneficial for users in choosing the best suited resource."
- "There is opportunity to increase the number of controls...Would be helpful to have additional controls, a stop gap between 108 controls and 800-53. Perhaps existing controls could be expanded to demonstrate levels of maturity."
- "We recommend consideration be given to refactoring NIST 800-161's approach to more explicitly map to the five CSF functions. We believe this will increase the ease of adoption across industry, and deliver more successful implementations of cohesive and integrated security programs."
- "Aligning job descriptions and team designations [that have been developed based on the NICE Framework] to the Core Functions of the NIST CSF could be an effective way for new programs to understand how to implement controls effectively."
- "[I]n our consulting, we leverage the NICE Framework and the CSF together as part of a holistic view into a cybersecurity risk management program."
- **"**Mapping the NIST CSF to other resources developed by the federal government."

2.2 Make it easier to understand how the CSF can be used with other cybersecurity guidance; provide more mappings with the NIST National Online Informative References Program (OLIR) and Informative References.

The CSF identifies a broad set of cybersecurity outcomes and includes informative references to existing standards, guidelines, and practices to provide additional implementation guidance. Commenters expressed interest in more mappings between the CSF and other resources. Since the publication of CSF 1.1, NIST has created the National Online Informative References (OLIR) Program, which provides an online, database-driven capability to document and share experts' understanding of the relationships between various standards and publications, including the CSF.

RFI Response Examples

- "NIST should consider using software to build a navigable NIST Cybersecurity Framework Ecosystem that could also link and show the relationship between the Cybersecurity Framework, the Risk Management Framework, and the Privacy Framework, as well as mappings, links, informative references, etc."
- "We recommend NIST develop a flow chart or road map that can help organizations connect all of these resources and recommendations and map them back to the CSF."
- "Modify NIST CSF to provide more granularity at, or below, the subcategory level"
- "NIST can improve the OLIR Program by increasing the number of informative reference documents included in the database as additional informative references are added to the Cybersecurity Framework. Additionally, NIST can include a description of the OLIR program in the Cybersecurity Framework to notify users of the Cybersecurity Framework of how to access additional informative reference documents."
- "One aspect that we had to 'DIY' was the inclusion of sector-specific regulations such as the FTC Safeguards…It may be helpful to incorporate these into informative references or to create a set of overlays that pull out the requirements from these documents and assign them to the five stages framework, so that users who are beholden to these regulations can simplify their compliance. However, we can also understand the view that sector-specific regulations belong in industry profiles and are not the purview of NIST."
- "Leveraging CSF subcategories may seem obvious until one investigates the supporting references that specify subcategory requirements…To remedy this, streamline references to better fit the subcategory and, consequently, to make the CSF easier to use."
- "NIST should work with industry to bring the informative references up to speed to reflect the latest cyber work products and thinking in this complex area."
- "A mapping of the three Risk Management tiers (implementation/operations level; business/process level, and senior executive level) and inclusion of NISTIR 8286 series references to the CSF Informative References would be helpful."
- "Recommend adding more robust mapping of controls and other frameworks. Many organizations either wish to or are bound by requirements to meet a variety of frameworks."

2.3 Address the important role of governance in cybersecurity risk management, although there are several different approaches for doing so.

The CSF has historically been valued as a process that supports coordination of cybersecurity activities through senior management of an enterprise. Currently, CSF 1.1 includes governance of cybersecurity risk management in the "How to Use the Framework" section, as part of establishing a cybersecurity program, and includes governance as a Category in the CSF Core. Comments referenced the importance of governance considerations in the CSF but offered different solutions on how to address governance in the CSF. Some comments requested that NIST elevate the role of governance to a new Function in the CSF Core, ensuring alignment of cybersecurity activities with enterprise risks and legal requirements, while others expressed support for separate guidance on governance. Other commenters suggested addressing governance by emphasizing enterprise risk management in addition to cybersecurity risk management.

RFI Response Examples

- "We encourage NIST to incorporate the appropriate role of governance functions and responsibilities into the CSF."
- "Formalizing a Governance Function would ensure audiences consuming maturity scores and reporting at the Function level consistently see reporting on this key area. It would also allow for additional focus on evolving areas of best practice, for example cybersecurity oversight."
- "…update the CSF to include the functions of 'Governance' and 'Supply Chain/Dependency Management'…"
- "…governance and executive leadership support has become a key cybersecurity topic…It should be noted that there are two frameworks already in existence that have a Governance function: NIST Privacy Framework and Cybersecurity Risk Institute Profile. We believe that Governance should be broken out into a separate function..."
- "NIST should align the CSF with its Integrating Cybersecurity and Enterprise Risk Management guidelines."
- "Given the CSF's success, [commenter] believes the CSF should serve as a model for risk management beyond cybersecurity. But the CSF should not itself be expanded to address noncyber risks because doing so could hinder its cyber-specific utility."
- "As NIST considers potential updates to the Framework itself, it should remember that the framework as it exists has been widely successful and should not seek to materially change the Framework Core. For example, many government dockets are contemplating including requirements on industry regarding governance and third-party risk. …[Commenter] believes that NIST should not include additional Functions on 'Governance' and 'Supply Chain/Dependency Management' at this time."

2.4 Improve alignment between the CSF and NIST privacy resources.

Commenters recognized the value that NIST privacy resources, including the NIST Privacy Framework, provide, such as building public trust. They saw value in NIST's coordinated approach to cybersecurity and privacy as exemplified by other publications such as Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5) and commented on the need for additional alignment or guidance when using the CSF in coordination with NIST's other frameworks to support privacy and cybersecurity risk management.

RFI Response Examples

- "NIST should continue and expand the focus upon privacy and individual liberties. Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities."
- "Given that NIST 800-53 SP Rev 5 has consolidated security and privacy controls for information systems, [commenter] believe[s] organizations can benefit from further guidance on how to use CSF in conjunction with the NIST Privacy Risk Management Framework (PRMF) to collectively address privacy and security risks. Providing guidance on creation of integrated current and target profiles and action plans utilizing both Frameworks, as well as integrated informative references in addition to existing CSF to PRMF crosswalks, can facilitate a broad approach to helping organizations reduce risks—whether privacy or security—to their operations and assets, which remains a challenge for many."
- "Additionally, [the commenter] propose[s] the following general principles to guide continued work on NIST's successful framework: [… A] strong regard for the security and privacy of end users builds trust in the companies with whom those end users choose to do business."
- "The [commenter] also thanks NIST for their extensive work on developing frameworks to address questions of privacy and artificial intelligence, as well. Given that many of these areas require robust cybersecurity protections as well, we encourage NIST to examine ways to further harmonize current and future frameworks to best integrate interconnected themes."
- "At a minimum, [commenter] believes that both the NIST Risk Management Framework and the NIST Privacy Framework should be incorporated into any revision of the CSF."
- "We found it helpful to have the CSF mapped to SP 800-53-5 as well as the Privacy Framework."
- "The revision is also an opportunity to provide alignment with existing NIST frameworks (e.g., privacy and risk)."

2.5 Engage with other federal agencies to ensure effective use of the CSF for policy, legal, and regulatory purposes.

Some of the responses noted that there are numerous ongoing cybersecurity policy and regulation discussions across various federal agencies. They suggested that the CSF may provide an opportunity to improve how organizations achieve and report adherence to those goals and requirements. In addition, commenters discussed the importance of aligning the CSF with efforts by other federal agencies.

RFI Response Examples

- "Future, and in development, U.S. government policies on cybersecurity should be aligned with the CSF and CSF 2.0. The U.S. government has many cybersecurity initiatives underway. No matter the vector of cybersecurity updates, from Executive Orders to legislation to agency specific regulation, there must be alignment with the CSF. The CSF should be leveraged to avoid duplication and fragmentation which only decreases overall security and readiness."
- "It would also be helpful if Federal agencies advanced common usage to the Framework."
- "By further aligning the Cybersecurity Framework with HIPAA, healthcare stakeholders will be better equipped to leverage sophisticated cybersecurity tools while ensuring regulatory compliance."
- "NIST may wish to consider an expanded approach to mandatory requirements. While the Framework itself would not impose such mandatory requirements, it should be drafted in such a way to permit this…"
- "Without clear relationships and hierarchy between materials created, the cybersecurity guidance space becomes crowded and potentially duplicative, and the relevance of the CSF is overshadowed by cyber regulations, especially if the regulations are not built on the CSF. Two timely examples, include the 2021 TSA Pipeline Security Directives and the first draft CISA Common Baseline Industrial Control System Performance Goals, which were not structured to align with the CSF."
- "[Commenter] supports NIST working with the National Telecommunications and Information Administration ('NTIA') as they fund broadband networks nationwide through the Infrastructure Investment and Jobs Act's Broadband Equity, Access, and Deployment ('BEAD') Program and utilize the revised framework to meet NTIA's cybersecurity and supply chain security goals for the program."
- "Current and in development programs like FedRAMP and the Cybersecurity Maturity Model Certification (CMMC) further complicate this issue for some organizations, raising questions about how these frameworks and certifications can align."

2.6 Increase international collaboration and engagement, including alignment with the ISO 27000 series.

The CSF Roadmap 1.1 recognized that "globalization and advances in technology have driven unprecedented increases in innovation, competitiveness, and economic growth." Commenters pointed out that, as governments around the world are proposing and enacting cybersecurity policies, laws, and regulations, it is imperative that the CSF (and NIST, in general) align with those initiatives. Commenters appreciated the efforts NIST has taken to position the CSF internationally and suggested NIST should continue to engage with international partners to increase integration with other international efforts and standards.

RFI Response Examples

- "[Commenter] hopes the CSF becomes truly globally common framework. [Commenter] applauds NIST's effort so far to position the CSF as a global framework, but there is still a way to go. This CSF revision process is a good opportunity to advance this objective, and [commenter] encourages NIST to reach out to international stakeholders as much as possible so that their opinions and voices are reflected and give them a strong stake in the outcome."
- "International engagement will be imperative to continue advancing efforts to improve cybersecurity globally and support a consistent approach to cybersecurity risk management. NIST should continue to participate in cyber dialogues led by the Department of State, commercial dialogues and other efforts led by the International Trade Administration, and in multilateral fora like APEC on cybersecurity and related topics to build upon its already robust international engagement efforts"
- "We encourage NIST and other U.S. government partners to increase investments in promoting the adoption and use of the Cybersecurity Framework both domestically and internationally."
- "NIST should identify the barriers to foreign adoption of the CSF 2.0 and tailor messaging and education to counter these barriers... NIST should conduct workshops with foreign governments and companies to identify different ways the CSF can be used and how it can integrate with other international standards."
- "The CSF should focus on international standards as base informative references wherever possible."
- "There is a lot of overlap in security recommendations between the Framework and other global standards, such as the ISO 27000-series and others. In addition, the Framework itself is adopted by organizations around the world. We encourage NIST to continue to engage in global outreach and align the Framework with other globally accepted standards."
- "…focus on international standards as base informative references."
- "This letter recommends that NIST update the informative references to RS.AN-5 to include standards that are directly related to coordinated vulnerability disclosure - specifically ISO/IEC 29147 and ISO/IEC 30111."

Theme 3: Offer more guidance for implementing the CSF.

3.1 Offer more guidance on CSF implementation.

Initially, NIST made the decision not to provide extensive implementation instructions for the nascent CSF. As reflected by the RFI responses, the security community – broadly including organizations that need to implement cybersecurity risk management measures – has developed innovative and diverse methods of applying the CSF and has incorporated the practices into products, assessment models, certifications, and more. Multiple comments pointed out, however, that the lack of specificity may result in inconsistent interpretation and implementation of the CSF. They reflected a desire for more implementation guidance, including more specific information about definitions, applications, and interoperability.

Other responses recognized that some CSF users may not be aware of guidelines and resources already produced by NIST and others. That led commenters to call for additional guidance, as well as improved awareness of available resources.

RFI Response Examples

- "While we appreciate the balance NIST aims to strike, we believe smaller organizations will need more prescriptive steps they can take if they are to improve their cyber posture."
- "Consider adding a 'Guidance' field to the CSF PDF and spreadsheet...add a 'Documents and Artifacts' field..."
- "…recommend NIST develop a best practices guide for using the Framework based on real use cases that successfully address the evolving threat landscape applying emerging cybersecurity concepts, principles and technologies."
- "Guidance is explicitly needed to address the minimum capability the organization must have to successfully adapt the Framework's guidance for implementing or improving cybersecurity capabilities. Many organizations that make up the critical infrastructure are small to medium-sized organizations with immature organizational capabilities."
- "The online learning content page should be more user-friendly and intuitive to navigate, including a simplified explanation of where to begin and how the standards work to supplement CSF."
- "…we recommend NIST consider developing a CF-type resource aimed specifically at smaller organizations with limited technical expertise in cybersecurity. This resource could focus on detailing, in non-technical terms, the various threats facing smaller organizations, proactive steps that could be taken to mitigate risks, actions to take should the organization experience a cyberattack, and contingency plans to ensure patient care is not disrupted."

3.2 Provide specific guidance on developing CSF profiles.

Respondents pointed out that the CSF Profile component is helpful, but the concept can be difficult to understand and apply. Comments suggested that, while NIST and others have provided examples of profiles for specific sectors, additional guidance on how to develop a profile (such as a template) would be helpful in facilitating use of the CSF.

RFI Response Examples

- "NIST has developed profiles that organizations can use to review aspects of their cybersecurity programs based on the elements and security objectives of the Framework… In refining the Cybersecurity Framework, NIST should describe how organizations can use Profiles and NIST's guiding principles of secure authentication, identity and access management to create desired targeted outcomes for different use cases, notably in supply chain security, IoT security, secure software development, and other issues relevant to various sectors."
- "NIST should consider how to amplify awareness and understanding of how to use sectoral and cloud profiles that leverage the Framework. While NIST provides links to such resources on both the 'Critical Infrastructure' and 'Example Profiles' tabs of the Risk Management Resources page, there's minimal context for understanding their purpose or supporting use."
- "The Profile is based on the …Cybersecurity Framework (CSF), but extended to include additional functions, control principles (called diagnostic statements), and regulatory references specific to the financial sector. … It is from this, in fact, that the Profile derives its name—it is a 'Framework Profile' based on guidance provided in the CSF. It is also an indicator of how the private sector and organizations can elaborate on the foundational work NIST has accomplished to date."
- "The framework likely does not intend to lay out a specific method to be used to create a profile or select implementations to achieve those outcomes in the profile (other than that it be based upon a risk assessment). Clarifying this point about what the framework does NOT intend to do, would make it clearer how to use the CSF together with other standards and guidelines that do intend to do those things."
- "[Commenter] also supports the development of starter framework profiles and other tools to simplify and streamline use of the Cybersecurity Framework."
- "There is also a lack of robust guidance in the current Framework around the Profiles and how to use them, including to explain how and when an organization should determine its current Tiers across Core practices or how it should develop a Current and Target profile."
- "[Commenter] recommends that NIST consider ways to make Section 2.2, Framework Implementing Tiers, and Section 2.3, Framework Profiles, more robust and useful to organizations."
- "…the framework is lacking a base profile that could be used to develop a Target Profile."

Theme 4: Ensure the CSF remains technology neutral but allows it to be readily applied to different technology issues – including new advances and practices.

4.1 Ensure the CSF remains technology neutral while providing guidance on how it is used to address cybersecurity risks in IT, OT, and IoT.

As directed by EO 13636, the CSF was originally designed for use by critical infrastructure providers, which rely heavily on industrial control systems and other types of operational technology (OT). Industry innovation continues to drive convergence of traditional IT, OT, IoT, and many other types of technology. Respondents recognized that the CSF would benefit from expanded discussion of that convergence, while cautioning NIST not to forego the existing technology-neutral stance. They shared that an updated CSF should be broadly applicable to all technologies.

RFI Response Examples

- "...it remains among the most important cybersecurity standards, both nationally and internationally. From an OT perspective, it has been very useful in outlining how and why the five functions are important in addressing the cybersecurity lifecycle for OT and ICT assets."
- "Although the Framework is not directly applicable to the management of risks for medical devices, our members have found portions of the Framework suitable to their management of cybersecurity risks."
- "NIST should avoid revising the Cybersecurity Framework to attempt to address the specifics for all cybersecurity risks…However, two areas that NIST should consider how to align more fully into the Framework are IoT and secure software development."
- "NIST should incorporate changes to the Framework Core to address cyber risk management associated with connected assets across IT, IoT, OT, mobile, container, and cloud environments."
- "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'."
- "NIST Guide to Industrial Control Systems (ICS): Security NIST Special Publication 800-82, should be mapped to NIST CSF. Cyber-physical security and process variable monitoring at the physical layer (ICS level 0-1) should be included in the NIST CSF."
- "Potential areas where NIST can add recommendations explicitly concerning IT/OT convergence include the following: asset management, risk assessment, and risk management strategy."
- "IoT devices present a clear and present risk to most business networks …NIST should integrate into its CSF an IoT template for standards and controls for critical infrastructure organizations."
- "Functions listed in the NIST Cybersecurity Framework should be expanded to take into account recent major cyberattacks focusing on data, such as data theft and cryptographic ransomware. Examples include tracking data movements across organizations to detect anomalies in data transfer, content inspection and data-centric risk assessment."

4.2 Consider the importance of software security, either as part of the CSF or in conjunction with the CSF.

Many responses called attention to the opportunity for CSF to better support software development and software supply chain considerations. Commenters reflected on the benefits of the guidance produced under Executive Order 14028, including the NIST Secure Software Development Framework (SSDF), and encouraged NIST to consider how secure software development practices relate to the CSF. Responses reflected a mixed opinion on whether to integrate SSDF and CSF.

RFI Response Examples

- "We encourage the use of NIST Special Publication (SP) 800-218, the Secure Software Development Framework (SSDF), as well as recognition of the need to incorporate practices into the Framework or issue guidance on how to use the SSDF along with the Framework."
- "The CSF needs more coverage for software/application development, from somewhere like the NIST Secure Software Development Framework or Google's SLSA Framework."
- "NIST may consider developing relationship mapping from the Framework Core to the Secure Software Development Framework's practices, tasks and implementation examples. We recommend NIST avoid the addition of software development specific descriptions to the Framework to the extent possible due to the importance of preserving the Framework as a flexible, and comprehensive cybersecurity risk management guidance."
- "We encourage NIST to consider mapping the categories and subcategories of the Framework to the Executive Order on Cybersecurity."
- "The [commenter] especially encourages NIST to consider how to incorporate secure software development practices into the Cybersecurity Framework."
- "NIST should add one or more explicit call-outs to the SSDF in the introductory text and Framework Core of the CSF (not just in the Informative References)."
- "The NIST Framework addresses cybersecurity for an operational organization and has minimal amount of content dedicated to developing secure software. Many organizations that use the Framework have substantial SW Development groups and are faced with adding another framework (e.g., SSDF or BSIMM) to cover all their related activities."
- "NIST should add cybersecurity strategy implementation guidance, as well as System Development Life Cycle guidance."
- "NIST should provide guidance on how the CSF should be applied alongside the Secure Software Development Framework (SSDF). One way to do this could be to map the SSDF Practices and Tasks as Informative References in the CSF."
- "Integrating software development, supply chain and metrics into the CSF should be done within the existing five top-level functions."

4.3 Ensure the CSF remains technology neutral yet can be applied to specific and emerging topics such as cloud, hybrid work, and zero trust.

Commenters recognized both the benefits and challenges of the CSF remaining technology-neutral through significant technical evolution. While many comments requested addressing specific topics, technologies, and applications in CSF updates (e.g., 5G Network Function Virtualization [NFV], quantum-resistant encryption, zero trust architecture), others cautioned against explicitly including specific topics and jeopardizing the broad applicability of the CSF across topics, technology, and applications. One area of broad agreement is that the CSF should more fully integrate cloud computing and shared service models in future updates.

RFI Response Examples

- "Since cybersecurity and its frameworks evolve from public-private collaboration, the cybersecurity community benefits from the CSF's unbiased, vendor-neutral approach..."
- "…update the CSF to include other items, such as encryption and key management, secure software development, cloud computing and shared services models, new technology adoption and operational resiliency to reflect the changing cyber and technology risk landscape."
- "Examples of such major shifts and changes are: global spread of remote-based working environment, increased digital connectivity across entities, increased inter-dependency across entities and sectors, availability of advanced network technologies (such as 5G), and advancement in digital technologies (such as encryption). Addressing these does not require that the NIST CSF should have solutions to all of these issues. Rather, by addressing these issues in the revision process, [Commenter] would hope for a more robust process and a more engaged set of global participants."
- "The use of the cloud and the specific risks that its use implies are not explicitly addressed. Although they can be considered in existing subcategories, it could be a topic to be dealt with specifically."
- "As [commenter] has indicated, however, the CSF is sorely lacking in practice area controls for cloud safeguards… The primary suggestion for the CSF would be just as there are specific CSF profiles for industry verticals, there should be specific profiles for practice areas."
- "[Commenter] recommends that NIST include Zero Trust efforts and taxonomy to stay ahead of the curve of Zero Trust implementations."
- "…ATT&CK provides an opportunity to characterize a threat actor's methods to inform a risk scenario, making it particularly relevant for the CSF functional categories of Risk Assessment (ID.RA) and Risk Management Strategy (ID.RM)."

Theme 5: Emphasize the importance of measurement, metrics, and evaluation in using the CSF.

5.1 Consider and highlight how the CSF is used as an assessment tool, including consider additional guidance on assessment (for self, suppliers, products, and services).

Respondents shared extensive and innovative approaches to using the CSF for assessment – both for internal self-assessment capability and as a methodology for external review. Further guidance and supplemental materials for using the CSF for self-assessment, external assessment, and auditing would be helpful, according to the responses. Some respondents recognized that it may not be practical for the CSF alone to be used for specific and detailed risk assessment purposes, although they identified value in using the CSF together with more specific risk management methodologies.

RFI Response Examples

- "…the NIST Cybersecurity Framework could allow for better assessment and management of risk if the gap between outcomes and the controls needed to address those outcomes can be related to an organization's unique risks and risk appetite and tolerances. That said, the level of analysis needed to address this issue is currently – and probably should remain – outside the scope of the Framework."
- "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."
- "Research that documents the use of specific elements of the CSF to security outcomes would be a strong lever for increasing the voluntary use of the NIST CSF."
- "Either self-assessing or getting an external assessment against the CSF requires significant resources. This itself is not a challenge but there could be more or better resources showing how organizations can implement the CSF in practice…"
- "We find the CSF's focus on all stages of the cybersecurity event lifecycle helpful in ensuring a comprehensive approach to evaluating maturity. To bring the CSF to life as part of our internal cyber maturity assessment program, [commenter] identified and mapped over 400 unique cyber capabilities to the 108 NIST CSF subcategories. Linking specific capabilities to each subcategory enables a consistent and complete approach when performing cyber maturity assessments over time."
- "NIST should educate organizations to apply the CSF accordingly as a tool for subjective identification of internal gaps but not as a tool for comparing scoring with other organizations."
- "[Commenter] members recommend additional guidance on assessment or maturity model mapping to the CSF to improve the usefulness of the CSF because it could be valuable to show the relationships between NIST guidance and other materials produced by government agencies."

5.2 Provide a means to measure CSF implementation.

As with previous RFIs, comments on drafts, and discussions at NIST forums, metrics and measurement remain a lively topic among respondents. Many recognize that cybersecurity program implementation and improvement is not a pass/fail exercise and that an effective program must be able to assess, coordinate, and report measurable activities. Many comments called for definition of specific metrics by subcategory; some also called for subcategories to be further decomposed to enable more specific measurement of specific activities. Others stated that such detailed metrics, such as specific control objectives, "defeat the broad applicability and flexibility that make the CSF valuable."

RFI Response Examples

- "We recommend...that NIST explicitly incorporate the importance of continuous monitoring, security ratings, and cybersecurity metrics into more of its documentation."
- "...measuring something as complex as cybersecurity is difficult but notes the inclusion of 'Measuring Cybersecurity' in the NIST Roadmap …and strongly supports increased investment in 'Research to understand challenges, insights, and gaps in cybersecurity measurement.'"
- "It is also not clear to some organizations how to measure the effectiveness of particular controls, and some of our members wondered whether it would be possible to determine which sets of controls actually result in fewer cyber incidents."
- "Today, there is a lack of insight for organizations on maturity within their respective industry and, as a result, where their organization stands in relation to others. Collaboration could be increased by facilitating an annual information sharing forum wherein organizations could present on their progress. In addition to an annual forum, NIST could consolidate and expand upon its 'Success Stories' and 'Perspectives on the Framework' pages for organizations to report on progress, successes, pain points, and other salient information."
- "[Commenter] recommends that the collection of metrics for improvements to cybersecurity as a result of the implementation of the CSF be considered in other risk management resources as they may present unintended compliance challenges. Given that the CSF is intended to be guidance, the collection of metrics on the alignment to the CSF is unwarranted without a meaningful rationale and material benefit for using metrics."
- "In essence, a new approach would begin with an updated NIST Framework to which entities would self-certify that they observed in their practices."
- "Suggested metrics for each of the core functions could be a great addition for the use of the NIST CSF. Development of metrics also prioritizes the components of a cybersecurity program."
- "Define measurement scales for each of the elements in the framework to reduce ambiguity and improve quality of benchmarking and measurement."

5.3 Expand on (or, in contrast, remove) Tiers and include (or do not include) guidance on maturity models.

Responses regarding Implementation Tiers were disparate. Some respondents pointed out that the use of Tiers needs more clarification. Some described the use of Tiers as a means to measure maturity of the cybersecurity program and implementation of specific capabilities, while others specifically thanked NIST for asserting that Tiers are not a maturity model. In general, many respondents stated it would be valuable to be able to measure process achievement for CSF outcomes, perhaps expressed through a maturity model. Comments also expressed that there may be value in aligning such a measurement capability with existing maturity models such as the Cybersecurity Capability Maturity Model (C2M2) and the Capability Maturity Model Integration (CMMI).

RFI Response Examples

- "The Tiers approach has some utility and can be further improved with some targeted refinement, but NIST should continue to be mindful of the risk that the Tiers may be used by some as a maturity model."
- "The CSF 1.1 is right to distinguish tiering from maturity; in contrast to a maturity model, Tiers can facilitate an organization's communication of its assessment of its cybersecurity risk management program into its broader risk management processes, which involve considerations about organization-wide priorities, resource availability and allocation, and risk tolerance, among other things."
- "There is opportunity to add risk ratings - High, moderate and low - Would help businesses prioritize remediation… Implement maturity level labeling within the CSF."
- "Consider adopting a tiered adoption model for CSF, like CMMC or CMMI."
- "We also encourage NIST to further build out guidance related to the Tiers. As referenced above, the Tiers are currently vague and challenging for many organizations to interpret."
- "…the implementation levels could be mapped to the subcategories, selecting which of these and under what conditions they allow to be placed in the different levels."
- "…the tier definitions do not imply that higher levels of security are achieved at higher tiers. They do imply that more appropriate levels of security are achieved at higher tiers. The level of security implemented might in fact become lower as the organization better understands and accepts their risk. In summary, the tier concept may be a useful management tool (though neither a maturity level nor a security level), but its logical connection and position as a key concept in the framework is not well explained."
- "An additional way NIST can improve the Cybersecurity Framework is by integrating a maturity model and/or assessment guidance that can assist organizations in understanding their position and progress in implementation efforts. Inclusion of this information and guidance can augment the implementation tiers already included in the CSF."

Theme 6: Consider cybersecurity risks in supply chains in the CSF.

6.1 Address supply chain risks, either in the CSF or separately.

Commenters agreed that supply chain risks represent an important element for many organizations. Many supported adapting the CSF to more fully cover cybersecurity supply chain risk management (C-SCRM) rather than creating a separate C-SCRM-specific framework. Several comments expressed concern that additional frameworks could cause confusion among implementing organizations.
RFI Response Examples

- "Supply chain should be manifested in additional places within the CSF; i.e., rather than just in the 'Identify' function, as now, to within the 'Respond' and 'Recover' functions as well."
- "CSCRM is like any other aspect of an organization's risk management program and should be integrated similarly into the NIST Cybersecurity Framework."
- "In a world in which cybersecurity challenges, risks, and impacts are increasingly felt across the entire network of the supply chain for a given product or service, however, it would be beneficial to consider augmenting the CSF to address these challenges and risks and identify new ways of managing and mitigating those risks."
- "Further integration of the framework with specific supply chain risk management standards may not be necessary. The voluntary, flexible approach of the framework should be retained. Prescriptive approaches for supply chain risk management should be avoided. Providing examples of supply chain risk profiles and references to additional supply chain resources might be more helpful."
- "By incorporating more supply chain risk management content into the CSF, the CSF can act as a guide to the relevant portions of NIST 800-161 for different categories and subcategories."
- "We recommend that NIST integrate CSF and Cybersecurity SCRM. This will avoid the burden of developing another framework and reduce confusion about use of existing resources. Given the increased importance of cybersecurity issues in the supply chain, we believe it should be an element in the CSF."
- "[Commenter] recommends that NIST update the Supply Chain Risk Management (ID.SC) informative references to include those references in particular that include the software supply chain work from the last four years."
- "NIST could integrate some supply chain risk management guidance into the NIST CSF but not interfere or conflict with existing compliance frameworks."
- "CSF should move towards incorporating similar SCRM controls, most notably SR-4-3, Identify as Genuine and Not Altered, SR-9, Tamper Resistance and Detection, and SR-11, Component Authenticity."

Theme 7: Use the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to align practices and provide effective practices, guidance, and tools to bolster cybersecurity supply chain risk management.

7.1 Align cybersecurity supply chain risk management practices, including federal activities and resources.

Commenters recognized the value of having a centralized source of information, best practices, and guidance regarding supply chain risk management. They shared that NIICS will provide that opportunity to integrate and align federal C-SCRM activities.

RFI Response Examples

- "We recommend that NIST consider and, where possible, harmonize the various government supply chain security initiatives through its NIICS efforts. Such alignment will help organizations adopt consistent supply chain cybersecurity principles within and across supply chains."
- "Even as more organizations recognize cybersecurity as a business imperative, leaders in many organizations still view cybersecurity as a cost center and/or lack awareness about how to cost effectively prioritize and address SCRM within their organization's missions. The NIICS can help address these challenges by: (1) driving awareness and education among organizational decisionmakers about the imperative value of SCRM to businesses and organizations of all types; (2) building understanding among organizational leaders about how to maximize SCRM investments (including through use of the Framework); and (3) coordinating with complementary federal initiatives to drive such education and awareness throughout the NIICS program."
- "While individual efforts towards addressing cybersecurity supply chain risk management (C-SCRM) continue to advance, there would be great value in unifying these efforts, much like the SECURE Technology Act and the Federal Acquisition Supply Chain Council, among other efforts, have recognized."
- "NIST [should] continue conducting multi-stakeholder engagements to define the National Initiative for Improving Cybersecurity in Supply Chains (NIICS). We … welcome the opportunity to participate in those engagements and look forward to collaborating and providing our open source security perspectives."
- "…security controls of the suppliers of the supplier should be communicated to the consumer. So just evaluating the immediate supplier's security controls will not be enough to assure security but being aware of the control strengths and weaknesses of the 4th or 5th parties will make the security due diligence complete and also help with better threat modelling and risk mitigation strategies."
- "NIST – working with sectoral agencies – to do more to promote and educate other regulatory authorities and critical infrastructure operators on the benefits of cloud, software and technology escrow solutions."

7.2 Offer more guidance on component inventories, such as software bill of materials and hardware bill of materials.

Numerous comments referenced the need for improved guidance and resources for asset management information including bills of materials (e.g., software bill of materials, or SBOM). They recognized that an important part of C-SCRM is understanding the hardware, software, and other component inventories used within the enterprise and within externally hosted environments.

RFI Response Examples

- "Identify additional guidance and standards needed to support agencies' consumption of SBOMs at scale, keeping in mind they are merely one element of software lifecycle management. Engage SBOM standards communities to provide guidance for software developers and agencies on how to produce and consume SBOMs."
- "By integrating the output hash of VSM into the SBOM standard as a record of the chain of evidence of software creation, an immutable record of the development process which can later be forensically examined. If the record on file does not match the cryptographically verified record from the software developer/creator, evidence of a problem exists that can be more closely examined for attribution. [Commenter] acknowledges that further development and research is required in this area to create a standard way to sign data to be certain of its provenance but early signs show promise in this area."
- "In addition to establishing a Software bill of materials (SBOM), a SaaSBOM for cloud services needs to be established. Part of the data flow for data identification and protection is knowing the cloud supply chain components of SaaS and other third-party applications."
- "The NIICS could reset the understanding and expectations of vendors by building on the current minimum elements for an SBOM work to provide prioritization and risk-based guidance on updated contract language and guide certification procedures for vendors and software to promote better cybersecurity practices."
- "A trusted, well understood hardware bill of materials (HBOM) would help with risk assessment, including cybersecurity vulnerabilities and supplier source identification."
- "Further, modalities could be explored to enhance transparency and security in software development process, for example, via a standardized Software Bill of Materials (SBOM)…A standardized SBOM with defined baseline attributes and standardized formats and identification schemes could go a long way in supporting this effort."

7.3 Engage on open-source software security issues.

The community provided feedback regarding the challenges presented by open-source projects and related software. Questions about supportability and security of these projects present supply chain risk challenges. For these reasons, commenters recommended that NIST could help engage with the open-source community to identify ways to address these and related challenges. Respondents also recommended that NIST develop more guidance regarding ways to balance the benefits of open-source software with the supply chain risk challenges.

RFI Response Examples

- "As an extension of investments in both the Framework and NIICS, we recommend that NIST considers the unique supply chain risk management challenges for organizations consuming (and producing) open source and provides guidance on how to tailor supply chain risk management processes to those scenarios. We recommend that NIST engage with open source communities… to develop and seek feedback on that guidance to ensure that it is feasible and reasonable."
- "NIST should consider developing a standard for developing and registering an approved list of open-source software/materials. There has been an increase in software supply chain attacks that exploit upstream open source ecosystems."
- "Identify ways to amplify efforts from open source communities and industry…to improve the security of open source projects and supply chains. This should include agencies evaluating their own use of open source and identifying how they can contribute to the security of this public good."
- "…the code portal may not currently adequately address the OSS lifecycle and enterprise usage. The OSS code portal could be further improved by adding a page dedicated to and expanding on OSS lifecycle and enterprise usage."

7.4 Offer more guidance on supplier relationship management and contracts.

In response to several questions regarding supply chain risks, many commenters pointed to the need for additional information and guidance for managing the suppliers themselves, and for developing sufficiently detailed contractual requirements. They pointed out that NIICS could provide guidance and templates for ensuring that security is appropriately specified and managed with suppliers.

RFI Response Examples

- "It is critical for organizations to actively manage the security of their upstream suppliers. With commercial suppliers, this is often achieved through contractual agreements, third-party certifications, audits, or other assessment and monitoring processes."
- "One approach that could be helpful is appropriate contract terms that protect both parties."
- "Managing supply chain risk should start with the careful selection and vetting of the vendor. Too many organizations do not adequately select and vet the vendors whom they ultimately retain."
- "Expanding The Supply Chain Risk Management Category and Creation of Contract Terms Beyond the Identify Function Could Be Valuable…Vendor and software management continue to be the greatest challenges because existing contract language may not align with cybersecurity requirements or may not support evolving industry practices. An extended Supply Chain Risk Management category will aid in resetting the understanding and expectations of vendors."
- "Security objectives and their related outputs, and measures should be included in supply chain contracts, including routine and continuous monitoring and as key topics in supply chain technical and management reviews."
- "Management of supplier transitions are especially important in systems of systems environments, from the onset of forming a supplier relationship."

7.5 There are opportunities for NIICS to research, analyze, and develop tools and techniques for better managing cybersecurity risks in supply chains.

Several respondents emphasized the important role that tools and techniques play in supporting cybersecurity supply chain risk management processes and procedures. As indicated by some of the examples provided, many of these tools and techniques support better management of cybersecurity risks in supply chains by providing automation, scalability, modeling, and data analytics for supply chain analysis.

RFI Response Examples

- "Emphasize the use of automated assessment tools…to continuously assess open source dependencies. Automated assessment tools shouldn't be used to govern whether a project should or shouldn't be used but instead to identify areas of risk that warrant deeper investigation and to measure improvement over time."
- "The rapidly growing IoT connectivity coupled with the lack of visibility in fragmented supply chains created opportunities and challenges which cannot be addressed by a single company. A collaborative, platform-based product design, delivery, and business ecosystem is needed in order to evolve an interoperable infrastructure for improving visibility among supply chains, market places, and end uses. Such platform can enable NIST to accelerate development of metrics and standards driven by the growth of data and analytics as a result of the increased visibility of the connected supply chain for microelectronics and IoT devices."
- "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."
- "Supply chain risk management solutions… can help identify, categorize, and maintain updated lists of qualified suppliers who can provide purchasers with recognized alternatives."
- "Managing cybersecurity-related risks in supply chains needs to be done at scale, leveraging automation to efficiently identify areas of risk that may take additional action."
- "Planning should be a continuous process, managing change to increase flexibility through new models, such as Supply Chain as a Service and systems that provide real-time, end-to-end transparency of software suppliers and the provenance of commercial and open-source software."