NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

January 19, 2023

Note to Reviewers

NIST is publishing this concept paper to seek additional input on the structure and direction of the Cybersecurity Framework (CSF or Framework) before crafting a draft of CSF 2.0. This concept paper outlines more significant potential changes that NIST is considering in developing CSF 2.0. These potential changes are informed by the extensive feedback received to date, including in response to the NIST Cybersecurity Request for Information (RFI) and the first workshop on CSF 2.0.

Some of the proposed changes outlined here are larger structural changes that may impact compatibility with CSF 1.1, thus warranting additional attention and discussion. This paper also outlines potential major changes to CSF resources, including the CSF website, Profiles, mappings, and guidance.

This paper *does not cover all* potential changes that may be made to the Framework structure, format, and content, especially specific changes to Categories and Subcategories of the CSF Core. NIST continues to welcome input on specific changes, including redlines, to the CSF narrative and Core, as well as to related CSF resources. NIST seeks feedback on this paper to inform further development of CSF 2.0, including, for each numbered section (e.g., Section 1.1. 'Change the CSF's title…'):

1. Do the proposed changes reflect the current cybersecurity landscape (standards, risks, and technologies)?
2. Are the proposed changes sufficient and appropriate? Are there other elements that should be considered under each area?
3. Do the proposed changes support different use cases in various sectors, types, and sizes of organizations (and with varied capabilities, resources, and technologies)?
4. Are there additional changes not covered here that should be considered?
5. For those using CSF 1.1, would the proposed changes affect continued adoption of the Framework, and how so?
6. For those not using the Framework, would the proposed changes affect the potential use of the Framework?

Feedback and comments should be directed to cyberframework@nist.gov by March 3, 2023. All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, or confidential business information should not be included. Comments with inappropriate language will not be considered. The changes proposed in this paper will also be discussed at the upcoming second CSF 2.0 virtual workshop on February 15, 2023, and during CSF 2.0 in-person working sessions on February 22-23, 2023. Contact cyberframework@nist.gov if you would like NIST to consider participating at a conference, webinar, or informal roundtable to discuss the CSF update and this paper.

After reviewing feedback on this concept paper and considering insights gained through the workshops, NIST intends to publish the draft Cybersecurity Framework 2.0 in the coming months for a 90-day public review.

Table of Contents

Introduction

The NIST Cybersecurity Framework (CSF or Framework) provides guidance to organizations to better understand, manage, reduce, and communicate cybersecurity risks. It is a foundational and essential resource used by all sectors around the world. Despite evolving cybersecurity risks, many respondents to the NIST Cybersecurity RFI reported that the CSF remains effective in addressing cybersecurity risks by facilitating governance and risk management programs and enhancing communication within and across organizations. The CSF has been adopted voluntarily and in governmental policies and mandates at all levels around the world, reflecting its enduring and flexible nature to transcend risks, sectors, technologies, and national borders.

The CSF is intended to be a living document that is refined and improved over time. The statutory authority for the CSF directs NIST to "facilitate and support the development" of the Framework and "coordinate closely and regularly" with relevant organizations.[1] With extensive community involvement, NIST initially produced the Framework in 2014 and updated it in 2018 with CSF 1.1. The CSF is being updated in an open manner with input from government, academia, and industry, including through workshops, public review and comment, and other forms of engagement. With this update, NIST is open to making more substantial changes than in the previous update. The "CSF 2.0" version reflects the evolving cybersecurity landscape—but community needs will drive the extent and content of the changes. An initial CSF 2.0 timeline is proposed in this figure:

The development of CSF 2.0 is iterative and based heavily on private and public sector input. Progress in the CSF 2.0 effort, as well as ways to engage, can be found on the NIST CSF 2.0 webpage. This paper is based off of feedback received thus far through:

- The 134 responses to the February 2022 NIST Cybersecurity RFI;
- The August 2022 "Journey to the NIST Cybersecurity Framework 2.0" Workshop #1, attended by almost 4,000 participants from 100 countries;
- Feedback from organizations that have leveraged the CSF; and
- NIST participation at conferences, webinars, roundtables, and meetings around the world.

[1] Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

Potential Significant Changes in CSF 2.0

This section outlines the proposed changes to the CSF 2.0 and related resources. NIST seeks feedback on each of the approaches described below. See the "Note to Reviewers" section above for additional details on submitting feedback to NIST.

In several of the sections below outlining proposed changes in the CSF and related activities, NIST identifies a "Call to Action" singling out ways in which the community can contribute to improvements to CSF 2.0 and associated resources.

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

While the CSF was originally developed to address the cybersecurity risks of critical infrastructure first and foremost, it has since been used much more widely. In recognition of this, CSF 2.0 will employ the broader and commonly used name, "Cybersecurity Framework" instead of the original "Framework for Improving Critical Infrastructure Cybersecurity."

The scope of CSF 2.0 will cover all organizations across government, industry, and academia, including but not limited to critical infrastructure. References to critical infrastructure in the CSF may be maintained as examples, but Framework text will be reviewed for broad applicability. Categories and Subcategories of the CSF Core that are specific to critical infrastructure, such as ID.BE-2 and ID.RM-3, will be broadened. This change is not intended to diminish the CSF's relevance to critical infrastructure organizations, including the importance of ensuring the security and resilience of our nation's critical infrastructure, but to embrace and enhance its broader use.

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

Since publication of CSF 1.1, Congress has explicitly directed NIST to consider small business concerns[2] and the cybersecurity needs of institutions of higher education[3] in the CSF. In addition, the CSF is a recognized resource for state and local organizations under the Department of Homeland Security (DHS) State and Local Cybersecurity Grant Program[4] and has been referred to widely by many associations as well as government agencies at multiple levels. Responding to the community's feedback and Congressional direction, NIST will increase its efforts to ensure the Framework is helpful to organizations – regardless of sector, type, or size – in addressing cybersecurity challenges and encourages all interested parties to participate in the process.

[2] NIST Small Business Cybersecurity Act (P.L. 115-236)
[3] CHIPS and Science Act (P.L. 117-167)
[4] Infrastructure Investments and Jobs Appropriations Act (P.L. 117-58)

1.3. Increase international collaboration and engagement

RFI responses called for increased international collaboration and engagement as an important theme for the CSF 2.0 update. Since the launch of the CSF's development in 2013, many organizations have made it clear that international use of the CSF would improve the efficiency and effectiveness of their cybersecurity efforts. The CSF 1.1 is frequently referenced in strategies, policies, and guidance developed by other nations. Several countries, across all regions of the world, have adopted or adapted the Framework, and some consider use of the Framework mandatory for their public and private sectors.

To facilitate international collaboration and engagement, NIST will prioritize exchanges with foreign governments and industry as part of CSF 2.0 development. NIST will continue to engage directly and through interagency partnerships to share the benefits of CSF use, as well as to solicit input on potential changes, so that the CSF can continue to be recognized as an international resource. NIST will also prioritize working with organizations to develop translations of CSF 2.0 in conjunction with its development, building on prior efforts to translate CSF 1.1 and relevant resources.

NIST will continue to participate in international standards activities that leverage the CSF as part of a broader effort and priority to engage strategically in the work of international standards developing organizations. This includes continuing ongoing work in the International Organization for Standardization (ISO) where several documents reference the CSF. NIST will continue to engage in the revision and development of cybersecurity risk management standards and guidance, as well as increase connections between these documents and the CSF.

NIST will also share information about its international engagement, as well as adaptations and translations of NIST resources via its International Cybersecurity and Privacy Resources site.

Call to Action – Share International Resources: NIST encourages the submission of international translations, adaptations, and other resources for the CSF.

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

Overwhelmingly, respondents to the RFI made clear that the Framework's key attributes – including its flexible, simple, and easy-to-use nature – have been beneficial for implementation by organizations of varying sizes, types, and sectors. Reflecting this input, NIST aims to maintain the current level of detail and specificity in CSF 2.0 to ensure it remains scalable and flexible for a wide range of organizations.

There is clearly recognized value in organizing cybersecurity outcomes by the CSF Functions, including providing context for more specific language commonly used in most cybersecurity standards. There is no shortage of cybersecurity standards, best practices, checklists, goals, and resources. The Framework will continue to provide a common organizing structure for multiple approaches to cybersecurity, including by leveraging and connecting to, but not replacing, globally recognized standards and guidelines.

2.2. Relate the CSF clearly to other NIST frameworks

Other NIST cybersecurity- and privacy-related frameworks – 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. Each focuses on specific topics worthy of dedicated guidance. However, as commenters pointed out, each framework has a relationship with the CSF, so they will be referenced as guidance either in CSF 2.0 or in companion materials, such as mappings. For example, CSF 1.1 was published prior to publication of the Privacy Framework; therefore, CSF Section 3.6, Methodology to Protect Privacy and Civil Liberties could be amended in CSF 2.0 to discuss how the Privacy Framework may be leveraged when implementing the CSF.

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

In addition to PDF and Excel formats, CSF 2.0 will be showcased through the recently launched NIST Cybersecurity and Privacy Reference Tool (CPRT). CPRT offers a consistent machine-readable format and user interface for accessing reference data from NIST cybersecurity and privacy standards, guidelines, and frameworks, as well as a flexible approach for characterizing the relationships between standards, guidelines, and frameworks as well as various applications and technology.

2.4. Use updatable, online Informative References

The CSF 1.1 Core identifies a broad set of cybersecurity outcomes based on and connected to Informative References – existing, widely accepted cybersecurity standards, guidelines, and practices to provide additional implementation guidance. While the concept of informative references was well received, some of the CSF's Informative References became outdated as those source documents were updated. In addition, the Informative References column in CSF 1.1 represents only a small subset of the example standards that may be leveraged by an organization in using the CSF. Many RFI commenters pointed to the value of the Informative References and expressed interest in additional mappings.

In CSF 2.0, NIST will move toward the use of online, updatable references showcased through CPRT. Since the publication of CSF 1.1, several resources have been mapped to the CSF beyond those included in the CSF 1.1 Core. For example, the Online Informative References Program (OLIR) Catalog contains approximately two dozen resources that are mapped to the CSF, including more recent versions of the Informative References included in the CSF 1.1 Core, as well as additional mappings not included in the CSF 1.1 Core. Further mappings, especially to sector-specific standards or specific use cases, can also be found in CSF sample Profiles and NIST publications, such as the Cybersecurity Practice Guides (SP 1800 series) published by the National Cybersecurity Center of Excellence (NCCoE).

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

NIST will work with the community to encourage and enable the production of mappings which support the CSF 2.0. There is strong community interest in additional mappings; respondents to the RFI requested mappings to almost 50 cybersecurity standards, guidelines, and other frameworks, many of which are authored by other organizations. With the use of online references, the CSF can be mapped to more specific resources to provide additional guidance,

such as those for securing controlled unclassified information, cloud computing, Internet of Things (IoT) and operational technology (OT) cybersecurity, zero trust architecture (ZTA), and more. In addition, it would allow for mappings for the CSF 2.0 at the Function and Category level, in addition to the Subcategory level, supporting connections to additional resources. The use of an online format can also allow mappings with greater description of the relationship between resources than currently included in the CSF Core.

Coupled with the addition of implementation examples (see 3.1), this should make it easier for users to find more guidance on how to meet CSF outcomes.

Call to Action – Provide Mappings: NIST welcomes submissions of mappings to the CSF. NIST encourages authors/owners of relevant cybersecurity resources to connect with NIST 1) to develop mappings to the CSF 1.1 if a mapping does not exist to ease the development of mappings to CSF 2.0, and 2) to coordinate releasing mappings to CSF 2.0.

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

CSF 2.0 will remain technology- and vendor-neutral. NIST recognizes that the technology landscape has changed significantly since the initial publication of the CSF. While RFI comments proposed that the Framework address specific topics, technologies, and applications in CSF updates, others cautioned against jeopardizing the broad applicability of the CSF. In order to remain technology-neutral, NIST will work to review the CSF so that its broad outcomes can continue to be leveraged by organizations regardless of the technology or services they employ, including IT, IoT, OT, and cloud services. Additional guidance on tailoring for specific technologies or applications may be best accomplished by CSF sample Profiles, mappings to specific standards or guidance (see 2.4 and 2.5), or implementation examples (see 3.1). The oversight of cybersecurity services, such as within cloud-hosted environments, will also be reviewed with the proposed expansion of governance (see 4.1) and supply chain risk management (see 5.1).

NIST is collaborating with the community to develop technology-specific mappings to describe the relationship between security capabilities that can be achieved by configuring or enabling security features within a technology stack and the desired outcomes described in the CSF. For example, the relationship between the CSF and Zero Trust Architecture (NIST SP 800-207) principles has been a frequent question raised by organizations. NIST is reviewing that relationship as part of the Zero Trust Architecture Project at the NIST NCCoE. Based on an initial mapping between ZTA characteristics and the CSF using the concept system mapping approach included in Volume E of "Implementing a Zero Trust Architecture" (NIST SP 1800-35E draft), NIST believes no changes to CSF Subcategories are needed in order to accommodate ZTA principles. ZTA capabilities support the outcomes outlined in the CSF to secure environments, although the implementation differs based on the technology composition. NIST encourages review and comments on this mapping in Volume E by February 6, 2023. Comments on this document may inform changes to the CSF. Other technology-specific CSF relationship mappings are being developed as part of other NCCoE projects, including Trusted IoT Device Network-Layer Onboarding and Lifecycle Management, 5G Cybersecurity, and Migration to Post-Quantum Cryptography, all of which may further inform CSF 2.0.

Given the importance of cybersecurity incident response, CSF 2.0 will expand consideration of outcomes in the CSF Respond and Recover Functions. The CSF must continue to emphasize the importance of incident response and recovery to maintain resilience and restoration of services. CSF 2.0 may include more consideration of response and recovery planning outcomes, increasing alignment with the popular Computer Security Incident Handling Guide, as well as leveraging the Guide for Cybersecurity Event Recovery. NIST encourages feedback about incident response and recovery outcomes that might be missing from the CSF that should be considered in CSF 2.0.

Identity management is also a critical cybersecurity topic. NIST is revising its Digital Identity Guidelines (NIST SP 800-63) with comments on the draft fourth revision open until March 24, 2023. In alignment with this revision, NIST will explore updates to the CSF's Identity Management, Authentication, and Access Control Category (PR.AC), including a potential re-ordering of Subcategories, to reflect the components of the digital identity model and phases of the digital identity lifecycle more clearly.

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

There were more than 500 references in the RFI responses 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. The call for additional guidance to assist organizations as they consider and use the CSF comes from a wide variety of organizations that have dramatically different needs and risks. Many would benefit from straightforward, more general descriptions of the Framework's key components, while others request detailed information such as linkages and mappings to specific cybersecurity guidance from NIST and other organizations. In conjunction with the development of CSF 2.0, NIST will address both needs using several approaches.

3.1. Add implementation examples for CSF Subcategories

CSF 2.0 will include *notional* implementation examples of concise, action-oriented processes and activities to help achieve the outcomes of the CSF Subcategories, in addition to the guidance provided in the CSF Informative References. Adding notional examples was suggested in the RFI responses and has been successfully leveraged in other NIST Frameworks such as the Secure Software Development Framework and the draft Artificial Intelligence Risk Management Framework Playbook. To ensure the CSF Core remains high-level and concise, there would be a small number of notional examples. This small list of examples would not be a comprehensive list of all actions that could be taken by an organization to meet CSF outcomes, nor would they represent a baseline of required actions to address cybersecurity risks.

There are many benefits to expanding and improving guidance for implementing the CSF by adding examples. These include helping to clarify the meaning and intent of each Subcategory and providing high-level implementation ideas within the CSF Core for those not as familiar with the detailed cybersecurity standards identified in the Informative References. 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.

Related CSF resources, such as CSF Profiles provided by NIST and other organizations and NIST Cybersecurity Practice Guides (SP 1800 series), could continue to cover further implementation examples to provide additional guidance for specific sectors, threats, or use cases.

NIST welcomes feedback as to whether these implementation examples should be added as a column included within the CSF Core (such as modeled after the Secure Software Development Framework), a column in the CSF Core highlighted in the Cybersecurity and Privacy Reference Tool, or in a companion guide separate from the CSF (as in the Playbook for the draft AI Risk Management Framework).

3.2. Develop a CSF Profile template

Many RFI responses called for additional guidance, including a template, for organizations to develop CSF Profiles. Framework Profiles are a way in which organizations implement the CSF by aligning the CSF's Functions, Categories, and Subcategories with the mission requirements, risk tolerance, and resources of an organization. Profiles also incorporate and align relevant informative references for Subcategories, including sector-specific standards and guidance and legal and regulatory requirements.

NIST has produced examples (and collected examples developed by others – including other federal agencies and associations) for several sector- and threat-specific Profiles that may be leveraged by an organization to build its organizational Profile. These sample Profiles make it easier for an organization to put the CSF into practice by prioritizing and aligning CSF outcomes with sector- and threat-specific risks and standards. Examples can be found on the NIST CSF website.

In conjunction with its development of CSF 2.0, NIST will produce an optional basic template for CSF Profiles suggesting a format and areas to be considered in Profiles. While organizations may continue to use different formats for Profiles based on their specific needs, use of a template is expected to increase the production of sector- and organization-specific Profiles and make the development of Profiles easier for users. NIST seeks feedback on what content should be leveraged in a CSF Profile template, including content organizations currently include in their CSF Profiles.

Call to Action – Share Example Profiles: NIST encourages private and public sector organizations to develop and share additional example Profiles for specific sectors, threats, and use cases, such as those identified on the NIST CSF website.

3.3. Improve the CSF website to highlight implementation resources

The NIST CSF website contains a wealth of information and additional guidance on implementing the CSF. These include numerous resources developed by NIST and external organizations, including CSF sample Profiles, mappings, guidance, tools, case studies, success stories, related publications (such as the CSF Quick Start Guide), and webinars. The update to the Framework presents an opportunity to increase awareness of these existing resources, as well as identify new ones. Accordingly, NIST will revamp the CSF website to refresh the content and enhance usability. As part of an ongoing review of the entire CSF website, NIST will remove

existing outmoded resources and add up-to-date resources. The site will be updated on a rolling basis during the CSF 2.0 update process. NIST invites feedback as to what additional resources should be developed by NIST or others to improve guidance to increase the ease and effectiveness of using the CSF.

To increase awareness, understanding, and use of the CSF, NIST has developed and worked with others to produce brief CSF Success Stories explaining how diverse organizations have used the CSF to improve their cybersecurity risk management. There is ample opportunity to expand the number of success stories as the current collection is limited – as indicated by the multitude of organizations which provide statements and indications of their productive use of the CSF.

Call to Action – Submit CSF Resources: NIST encourages organizations to submit to NIST recently published resources pertaining to the CSF for inclusion in the resource repository on the CSF website. These can include approaches, implementation guides, mappings, case studies, tools, and others. Please review the criteria for inclusion on the CSF website.

Call to Action – Share Success Stories: NIST will place a greater emphasis on success stories and reinforce that it encourages organizations to prepare and submit to NIST for consideration their own success story so that they may serve as a use case for NIST and others to understand how organizations are using the CSF to better manage and reduce their cybersecurity risks.

4. CSF 2.0 will emphasize the importance of cybersecurity governance

Cybersecurity governance is currently addressed in CSF 1.1 in the "Identify" Function, as well as in the section on "How to Use the Framework." CSF 2.0 will expand the consideration of these topics.

4.1. Add a new Govern Function

Reflecting substantial input to NIST, CSF 2.0 will include a new "Govern" Function to emphasize cybersecurity risk management governance outcomes. While the five CSF Functions have gained widespread adoption in national and international policies, including ISO standards, NIST believes that there are many benefits to expanding the consideration of governance in CSF 2.0. This new crosscutting Function will highlight that cybersecurity governance is critical to managing and reducing cybersecurity risk. Cybersecurity governance may include determination of priorities and risk tolerances of the organization, customers, and larger society; assessment of cybersecurity risks and impacts; establishment of cybersecurity policies and procedures; and understanding of cybersecurity roles and responsibilities. These activities are critical to identifying, protecting, detecting, responding, and recovering across the organization, as well as in overseeing others who carry out cybersecurity activities for the organization, including within the supply chain of an organization. Elevating governance activities to a Function would also promote alignment of cybersecurity activities with enterprise risks and legal requirements.

The new Govern Function in CSF 2.0 will inform and support the other Functions. CSF 1.1's inclusion of governance considerations in the Identify Function has created overlap between the cybersecurity risk governance and risk management activities of the Framework; this separation will make clear that governance outcomes inform the prioritization and implementation of each

of the current Functions. A crosscutting Govern Function is also consistent with the Govern Functions in the draft AI Risk Management Framework and the Privacy Framework.

The current Categories in the CSF 1.1 that cover governance would be moved into the new Govern Function. NIST requests feedback as to which current Categories should be moved. These could include Business Environment (ID.BE), Governance (ID.GV), and Risk Management Strategy (ID.RM).

CSF 2.0 will also expand consideration of governance-related topics in the new Function. For example, the current subcategories under Governance (ID.GV) – such as cybersecurity policy (ID.GV-1), cybersecurity roles and responsibilities (ID.GV-2), legal and regulatory requirements (ID.GV-3), and governance and risk management processes (ID.GV-4) – could each be elevated to separate categories under Govern. NIST welcomes input about what Categories and Subcategories should be incorporated in this Function. NIST will review other NIST frameworks with governance as an existing function to see if any of the categories are applicable for inclusion in the CSF 2.0. For example, this review will include the Govern categories from the NIST Privacy Framework, the Cyber Risk Institute's The Profile (financial sector CSF Profile), the draft NIST Information and Communications Technology Risk Outcomes (SP 800-221A), and the draft AI Risk Management Framework.

4.2. Improve discussion of relationship to risk management

Revising the CSF offers an opportunity to clarify the relationship among governance and cybersecurity risk management across the CSF narrative and Core. CSF 2.0 will describe how an underlying risk management process is essential for identifying, analyzing, prioritizing, responding to, and monitoring risks, how CSF outcomes support risk response decisions (accept, mitigate, transfer, avoid), and various examples of risk management processes (e.g., Risk Management Framework, ISO 31000) that can be used to underpin CSF implementations.

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

5.1. Expand coverage of supply chain

RFI respondents agreed that cybersecurity risks in supply chains and third parties are a top risk across organizations. While respondents largely agreed that NIST should not develop a separate Framework to address these risks, they were mixed in how this concern should be addressed in the CSF update.

Managing cybersecurity within the supply chain was one of the key additions in the last update to the CSF. Since then, even more attention has been paid to developing guidance to increase trust and assurance in technology products and services, including guidance developed pursuant to the Executive Order, "Improving the Nation's Cybersecurity" (EO 14028). CSF 1.1 added the CSF "Supply Chain Risk Management" (ID.SC) Category; expanded Section 3.3, Communicating Cybersecurity Requirements with Stakeholders to better understand C-SCRM; added a new Section 3.4, Buying Decisions to highlight the use of the Framework in understanding risks associated with off-the-shelf products and services; and incorporated C-SCRM criteria into CSF Tiers. In addition, third-party management is included as a consideration as part of broader CSF outcomes across the Framework Functions.

Given the increasing globalization, outsourcing, and expansion of the use of technology services (such as cloud computing), CSF 2.0 should make clear the importance of organizations identifying, assessing, and managing both first- and third-party risks. However, third-party risks may involve distinct assessment and oversight that is often handled by separate teams/organizations. Thus, NIST believes CSF 2.0 should include additional C-SCRM-specific outcomes to provide additional guidance to help organizations address these distinct risks. NIST invites feedback as to how best to address C-SCRM in CSF 2.0. Options may include: 1) further integrating C-SCRM outcomes throughout the CSF Core across Functions (integration may include supply chain separately or as a consideration as part of broader outcomes), 2) creation of a new Function focused on outcomes related to oversight and management of C-SCRM, or 3) expanding C-SCRM outcomes within the current ID.SC Category in the Identify Function.

In addition, since the release of CSF 1.1, NIST has developed the Secure Software Development Framework, recently updated pursuant to EO 14028. NIST invites feedback in the potential treatment of secure software development as part of the treatment of C-SCRM outcomes.

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

Measurement and assessment of cybersecurity risk management programs and strategies continues to be an important area in the use of the CSF. The RFI responses indicate respondents seek additional CSF guidance and resources to support measurement and assessment of an organization's use of the CSF. A related desire is for the CSF to clearly explain how organizations can use the Implementation Tiers, and how they relate to measurement.

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

CSF 2.0 will make clear that by leveraging the CSF, organizations have a common taxonomy and lexicon to communicate the outcome of their measurement and assessment efforts, regardless of the underlying risk management process. Across all organizations, a primary goal of cybersecurity measurement and assessment is to determine how well they are managing cybersecurity risk, and if and how they are continuously improving. The activities supporting measurement and assessment – from system-level to organization-wide – are inputs to determining maturity and supporting risk management decisions.

6.2. Provide examples of measurement and assessment using the CSF

Each organization's risks, priorities, and systems are unique, so the methods and actions used to achieve the outcomes described by the Framework Core vary. As such, measurement and assessment of outcomes vary depending on the context. Because there is no single approach to measure and assess the CSF, NIST will not put forward a single approach to assessment in the CSF 2.0 in order to continue flexibility in how organizations may implement the Framework.

Instead of one approach, CSF 2.0 will include examples of how organizations have used the CSF to assess and communicate their cybersecurity capabilities. This may include examples of how organizations can leverage the CSF, combined with risk management strategies and maturity models, to communicate answers to questions about the effectiveness of their cybersecurity

program. These include: What is the best way to communicate organizational cybersecurity posture to non-cybersecurity audiences? Is the organization's cybersecurity maturity improving? Where does the organization need to improve? How does an organization understand its cybersecurity posture across the organization, aggregating across systems?

CSF 2.0 Workshop #1 panelists provided a start by offering examples of how organizations have assessed use of the CSF by leveraging other risk management frameworks and maturity models; each organization aligned their CSF implementation with specific mission or business needs.

Call to Action – Share Use of the CSF in Measuring and Assessing Cybersecurity: NIST encourages organizations to share information with NIST about how they are using the CSF to measure and assess their cybersecurity. In addition, NIST encourages organizations to share information with NIST about the use of CSF Tiers. Relevant use cases could be incorporated into the CSF or provided as separate resources for additional implementation guidance.

Measurement Terminology: NIST is providing background on measurement-related terminology to help facilitate shared understanding of these topics to improve feedback on this paper, as well as discussion at the upcoming workshop. Terms and concepts around cybersecurity measurement vary greatly and ultimately are driven based on the context in which they are used. Formal definitions of these terms can be found in the draft Performance Measurement Guide for Information Security, which is open for public comment.

Assessment – The action of evaluating, estimating, or judging against defined criteria. Assessment approaches can be qualitative, quantitative, or semi-quantitative. Examples of types of assessments include risk assessment and control assessment.

For example, risk assessment can leverage risk matrices with colored rating scales to show likelihood and impact (qualitative assessment approach), number of known vulnerabilities in a system or organization (quantitative assessment approach), or a representative numerical scale (e.g., 1-10) to indicate severity of a risk (semi-quantitative assessment approach).

Measurement – The process of obtaining one or more quantitative values.

For example, number of phishing attempts averted through cybersecurity training and awareness.

Metrics – Designed to i) facilitate decision-making; and ii) improve performance and accountability through collecting, analyzing, and reporting relevant performance-related data. Metrics are used to track, compare, and assess performance or processes and are tied to a goal or performance requirement.

For example, a cybersecurity training effectiveness metric is having 80% of users report known phishing attempts.

6.3. Update the NIST Performance Measurement Guide for Information Security

NIST is updating its flagship measurement guidance document, the Performance Measurement Guide for Information Security. SP 800-55r2 provides guidance to organizations on the use of measures to improve decision making, performance, and accountability of a cybersecurity program or information system. This guidance applies to the measurement of multiple cybersecurity program activities, but given the interest in measurement associated with CSF 2.0, it may be especially useful for those who leverage the CSF. The underlying fundamentals of cybersecurity measurement process and implementation will not be included in the CSF, but rather in NIST SP 800-55.

Call to Action – Comment on Performance Measurement Guide for Information Security: The comment period for the working draft outline of SP 800-55r2 is open through February 13, 2023. Comments on this document may inform the discussion of measurement and assessment in CSF 2.0.

6.4. Provide additional guidance on Framework Implementation Tiers

The CSF Tiers provide a mechanism for organizations to view and understand their approach to cybersecurity risk and the processes and programs in place to manage that risk. The Tiers have an increasing degree of rigor and sophistication in describing overall cybersecurity risk management practices, including the risk management process, risk management program integration, and active participation in the wider cybersecurity ecosystem. Feedback from the RFI and workshop indicate organizations are using Tiers in a variety of ways and for different purposes to allow for flexibility in implementation, as originally designed. Examples of implementation range from helping to set internal goals and prioritize specific cybersecurity capabilities to communicating an organizational cybersecurity posture and helping measure the maturity of cybersecurity programs as well as the implementation of CSF outcomes at the CSF Function, Category, and Subcategory level. NIST invites continued feedback on how organizations are using Tiers, noting the request for greater clarity about Tiers and to ensure that CSF 2.0 reflects a variety of approaches.

CSF 2.0 will clarify the scope and applicability of Tiers to address robustness of risk management processes, programs, and external communication. The update will also better describe the relationship between Tiers and maturity model concepts, but consistent with the approach described broadly to address cybersecurity measurement (see 6.2), CSF 2.0 will not provide a distinct maturity model to meet CSF outcomes at the Function, Category, or Subcategory level. Supplemental resources could include new guidance of how the Tiers can be used in CSF Profiles, and increased focus on resources for the community to share mappings among Tiers, risk management processes, and maturity models.

NIST seeks additional feedback to determine the value of shifting the focus of Tiers to goals and objectives in the context of governance, including whether Tiers should continue to include the concept of “external participation,” or if Tiers could serve as a qualitative assessment approach that could be incorporated into or based on the outcomes of the new proposed Govern Function.