Initial Analysis of Responses to Request for Comment (RFC) on Cybersecurity Framework Version 1.1 Draft Update

Applied Cybersecurity Division, Information Technology Laboratory
National Institute of Standards and Technology (NIST)
May 15, 2017

1. Introduction

Version 1.0 of the "Framework for Improving Critical Infrastructure Cybersecurity" was prepared by the National Institute of Standards and Technology (NIST) with extensive private sector input and issued in February 2014. The voluntary Framework was developed in response to Presidential Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, which was issued in 2013. The Cybersecurity Enhancement Act of 2014[1] (CEA, Public Law 113-274) formally updated NIST's role to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure (CI) owners and operators. CEA calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure, in close coordination with critical infrastructure owners and operators.

NIST continues to collaborate with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework, which is based on existing standards, guidelines, and practices. It provides a repeatable, flexible, and cost-effective means for critical infrastructure to identify, assess, and manage cybersecurity risk. It is increasingly being used on a voluntary basis by many organizations across the United States and is also finding applications in other countries.

On January 10, 2017, NIST issued a draft update[2] of the Framework. This update sought to clarify, refine, and enhance the Framework, while minimizing disruption to current and potential users. Changes found in the draft update are based on:

- Feedback to NIST since the release of Framework Version 1.0 in February 2014,
- Responses to the December 2015 Request for Information[3],
- Comments provided by approximately 800 attendees at an April 2016 Workshop[4],
- Advances made in areas identified in the Roadmap[5], and
- Shared resources from industry stakeholders[6].

[1] [PDF] https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf
[2] [LINK] https://www.nist.gov/cyberframework/draft-version-11
[3] [LINK] https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity
[4] [LINK] https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016
[5] [PDF] https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf
[6] [LINK] https://www.nist.gov/cyberframework/industry-resources

When NIST issued the draft update, it also published a request for comments (RFC)[7]. This document represents an initial, high-level analysis of the 129 RFC responses NIST received. Those responses included many comments registered on behalf of multiple organizations.

This analysis will serve as a starting point for discussions at the May 16-17, 2017 Cybersecurity Framework Workshop[8]. Participants in that workshop and others are invited to evaluate the themes identified by NIST, determine if these themes reflect comments received through the RFC, and assist where additional stakeholder engagement will be needed to guide the Framework update process.

2. Methodology

NIST analyzed each RFC response to:

- Determine *basic respondent information*, including sector, size, and organization type;
- Identify *which sections* of the Framework or topics of the Roadmap the response addresses;
- Identify *key points,* commonalities, and recurring language across all respondents – which contributed to the development of themes.

Examples of respondents' quotes were associated with the themes. NIST augmented each theme with Representative Questions for discussion at the Cybersecurity Framework Workshop.

3. Themes from RFC Analysis

An outline of themes and several of the sub-themes follows:

Labeling of the Framework

- Revisions to the title of the Framework to delete "critical infrastructure" would convey that it is useful more broadly

Section 2.2 Tiers

- Continued refinement and clarification of the value and use of Implementation Tiers is needed
- Additional guidance or use cases on the Implementation Tiers would be helpful

Addition of Supply Chain Risk Management (SCRM)

- The addition of SCRM to the Framework is generally viewed as positive and needed
- Additional examples, use cases, and references would be helpful to further clarify SCRM use in the Framework

Section 4.0 Measuring and Demonstrating Cybersecurity

- The addition of a measurement section was deemed important by many, with further development of the measurement section recommended
- The measurement section should be labeled to clearly indicate that measurement provisions should be for internal or self-assessment use
- Care should be taken to ensure continued risk-based application of the Cybersecurity Framework and to avoid compliance-based application
- Recommendations were made about categories of measurement

[7] [LINK] https://www.federalregister.gov/documents/2017/01/25/2017-01599/proposed-update-to-the-framework-for-improving-critical-infrastructure-cybersecurity
[8] [LINK] https://www.nist.gov/news-events/events/2017/05/cybersecurity-framework-workshop-2017

- Some suggested less emphasis on quantitative measurement

Appendix A: Framework Core

- Respondents affirmed the integration of SCRM into the Core. Some respondents suggested SCRM be integrated across existing Categories, rather than adding an SCRM Category to the Identify Function
- Respondents affirmed the enhancement of the Identity Management, Authentication and Access Control Category and provided further thoughts for consideration
- Modifying and improving the usefulness of Informative References is appropriate, and the process for determining future Informative References should be defined

Small Business Prioritization

- NIST should continue to support Small Business involvement with the Framework and provide greater clarity about how smaller businesses can use the Framework.

Global Outreach Efforts

- Continue to promote the Framework internationally in the interest of alignment and common approach.

Revisions to the title of the Framework to delete "critical infrastructure" would convey that it is useful more broadly

RFC Response Examples:

- The label "Version 1.1" is adequate, but we suggest removing "Critical Infrastructure" from the title "Framework for Improving Critical Infrastructure Cybersecurity" and titling the document simply, "The Cybersecurity Framework." While we understand the name's origins come from Executive Order 13636, which initiated its creation, the use and value of the Framework stretches beyond critical infrastructure owners and operators. The short, straightforward "The Cybersecurity Framework" is memorable, rolls off the tongue well, and captures the broad scope.
- Removing "critical infrastructure" from the title will signal that this is a generally applicable guidance document that offers resources to companies at every stage of cybersecurity policy development. Framing this document more broadly could lead to wider adoption among small businesses and organizations in the United States and abroad.
- Industry sectors included in the critical infrastructure are specifically listed. While this identification of the industry sectors is important, there is some confusion as to what enterprises within those sectors are part of the critical infrastructure. Some appear to follow a very broad interpretation and believe that every enterprise within these sectors is part of the critical infrastructure. Others tend to prefer a more narrow interpretation and include in the critical infrastructure only the most important enterprises within these sectors. They point out that, for example, a small one-person insurance agency probably should not be classified as part of the critical infrastructure simply because it is part of the banking and finance sector. In the absence of guidance, it may be difficult to draw the line at the appropriate place.
- Version 1.1 is an appropriate label for this update. In promoting international awareness of the Framework and NIST's approach to public-private partnership, U.S. Government agencies and NIST should demonstrate the significant continuity between Version 1.0 and Version 1.1.
- The proposed update to the NIST Cybersecurity Framework minimizes disruption for institutions already using the Framework by maintaining the existing Core structure (i.e., Functions, Categories, and Subcategories), the document sections (i.e., Framework Introduction, Framework Basics, How to Use the Framework, and Appendices), and overall language introduced in the version 1.0. Given the limited magnitude of changes brought to the version 1.0, the label "version 1.1" is adequate.
- With respect to the name for the Framework update, we believe "Version 1.1" hits the mark as it is more appropriately reflective of refinement, rather than the type of major revisions "Version 2.0" might imply.
- "Version" numbers are typically applied to software. Consider the use of editions, rather than versions, since this is more common for recording changes to documents (i.e., first edition, second edition, etc.)

Representative Questions:

- Would a title change lead to additional use domestically and internationally?
- Would deletion of the reference to "critical infrastructure" reduce its use by those sectors?
- What is an appropriate label for the proposed update?

Continued refinement and clarification of the value and use of Implementation Tiers is needed

RFC Response Examples:

- [The Organization] respect[s] the changes that they tried to make to the tiers, but we expect that industry will still not understand how to use them and what the relationship is with the profiles.
- [The Organization] believes that additional clarity around the purposes of the Implementation Tiers and the tools that organizations can use to move from one tier to another will facilitate adoption of the Framework and thereby increase its use across various industry sectors.
- [The Organization] also encourages NIST to further clarify the criteria for designation at each of the given Tiers. As we noted in our earlier comments, the risk management process description for Tier 2 and Tier 3 are remarkably similar, making it difficult for companies to distinguish between the Tiers in practice. Removing this ambiguity would make the Framework more useful, which would likely further boost adoption by the business community.
- Consistency of content could be improved across different sections. For example, the descriptions of each Tier vary, which can make it difficult for some readers to understand the elements between them that make a difference and to determine how to progress from one Tier to the next.
- There continues to be misperception and a lack of clarity about the use or value of implementation Tiers. The addition of Cyber Supply Chain Risk Management to the Tier descriptions adds complexity to Tier designation. Added complexity risks organizations moving away from making decisions based on a risk management approach to a compliance-based checklist application of Tiers based on a maturity model, such as CMMI. NIST might consider removing implementation Tiers as a "core" component of the Framework, leaving it to each organization to apply Tier-like requirements to their individual or industry Framework Profiles.
- Prior to Draft Version 1.1, criteria within the Implementation Tiers have focused on attributes of maturity that cut across topics, rather than including specific topical or domain areas; the topic and domain areas have instead been built into the Core. As we have advocated for in previous feedback to NIST on the Framework, greater clarity around the distinctions between adjacent Implementation Tiers would increase usability.
- We believe SCRM should not be included in the Tiers at all. Supply Chain Risk Management is a component of an organization's Risk Management Process and Integrated Risk Management Program, both of which are components of all current Tier definitions. There is no need to call out individual components in the Tiers. If done in this manner, the Tier definitions could become bloated and complex, neither of which is a desirable outcome.

Representative Questions:

- For those who found Tiers useful, how did you use them? Did you find outside resources helpful?
- For those who have not found the Tiers useful, how did you attempt to use them, and what was the specific challenge?
- Why should SCRM, or any other dimension, be included in the Implementation Tiers? What do we consider qualifying criteria?

Additional guidance or use cases on the Implementation Tiers would be helpful.

RFC Response Examples:

- Documentation explaining the Tiers needs to be expanded and clarified. As the original version did, the Framework uses the verbiage in the Tiers to describe itself, i.e. the definition is self-referencing. There needs to be a clearer explanation of the Tiers and their value to the overall evaluation process.
- We advise including use case scenarios to describe the intended implementation and outcome of the Implementation Tiers at the organizational and sectoral levels to clarify proper application. This will help flesh out requirements that are applicable to a particular use case or intended outcome scenario and help to avoid situations where conceptual constructs may be value add in theory, but where actual practice may not yield the intended outcome in implementation (e.g. FISMA certification and accreditation process for information systems and FISMA scorecard, which have either evolved or have been deprecated).
- Guidance on how to ascertain control tier needs. I've helped small businesses implement CSF, and I've made an informed information security decision for them on what an appropriate tier would be (for their current size, business, needs), but I feel there is a gap there if the business is trying to adopt without a security professional to assist.
- Our only recommendation here (tiers) would be to add an appendix with a sample profile and describe the relationship in the tier for the example use case. (Users have a desire to see/know what "correct use" looks like, whether through examples, templates, published use cases, etc.).
- [The Organization] proposes that NIST provide more granular guidance on how to implement the Framework tiers and, just as importantly, "how", "why", and "when" organizations should advance from one Framework tier to the next.
- We do believe further clarifying guidance is warranted to make clear the Tiers are primarily intended to be used by organizations for internal purposes. [The Organization] previously commented that, without a common methodology for how tiers are determined and without a statement on the scope of how they may be used, in particular by external parties, the tiers could create unintended anticompetitive consequences.
- Several updates have been made to clarify the objectives and usage of Implementation Tiers, but [The Organization] believes additional guidelines should be provided to support effective leverage in combination with Profiles and the Core.

Representative Questions:

- Does the material on the Industry Resources page help those who are looking for Use Cases and Guidance on the Implementation Tiers?
- Are there other places where use cases and guidance is available? If so, where?
- How many different ways do you use the Implementation Tiers?

Addition of Supply Chain Risk Management (SCRM) to the Framework is generally viewed as positive and needed

RFC Response Examples:

- [The Organization] appreciates NIST's recognition of growing threats against the private sector and encourages additional focus on risks stemming from interdependencies with third parties: We support the continued focus on cybersecurity threats against the private sector. Our nation's businesses are increasingly on the front lines of sophisticated cyber threats that attempt to steal our intellectual property and undermine confidence in our economy. Our national economic security depends on U.S. enterprises' network defenses to safeguard systems and data and to provide secure and resilient services. However, our businesses also depend on global supply chains and third parties to provide our products and services. As a result, our risk assessments need to account for evaluating and measuring risks that come from third parties. Therefore, we support NIST's expansion of the focus of the Framework to include third-party relationship risk management.
- [The Organization] supports the addition of a cyber supply chain risk management category in the Identify Function of the Framework Core as it reflects a key risk factor facing critical infrastructure organizations, and multiple other organizations. However, [The Organization] would recommend against any further additions to the Core regarding cyber supply chain risk management until the standards landscape develops further in this space.
- [The Organization] supports the inclusion of SCRM in the updated Framework. [The Organization] believes that the discussion of SCRM activities and explaining how the updated Framework can be used to make risk-informed buying decisions by identifying security priorities and residual security risk adds significant clarity around how organizations can use the Framework to improve their SCRM.
- [The Organization] appreciates NIST's effort to provide a common taxonomy for supply chain risk management ("SCRM"). But the current draft dives into a discussion of SCRM without providing adequate context. The draft could be improved by adding a section at the beginning of Section 3.3 that describes the basics of SCRM.
- [The Organization] is pleased to see this draft of the CSF posted for comment and is encouraged to see the additions related to supply chain risk management. The CSF provides useful guidance and we encourage its broad use and adoption. Including supply chain risk management is timely and an important move forward for the CSF as it reflects a crucial source of risk.
- Members agree that the new content on Supply Chain is quite useful. Some [sic] members handle critical data of customers and call out a specific set of supply chain activities for their clients and risk management. There is concern, though, as to the precedent set by making Supply Chain a category. Supply Chain, much like "cloud", "internet of things", "mobility" and other themes, can be considered as a "lens", providing context for thinking about cybersecurity. Adding such items as categories replicates common sub-categories (risk assessment for "cloud", "internet of things", and "mobility", "contracts" for "cloud" and "mobility", etc.) and thereby grows the Framework core needlessly.

Representative Questions

- How do you address the cybersecurity dimensions of external relationships within your organization? Is that function labeled SCRM or something else? Is that function inclusive of contractual relationships and non-contractual relationships?
- Is the entity taxonomy in Section 3.3 helpful and reflective of your SCRM experiences? If not, how should it be evolved? Is the process described in Section 3.3 helpful and reflective of your SCRM experiences? If not, how might it be modified?
- How should any significant topic, including SCRM, be incorporated into the Framework? Does it deserve to be treated as a category of its own?
- Assuming that SCRM remains in the final version of 1.1, should it be removed from the Roadmap? If not, what additional work is needed on SCRM?

Additional examples, use cases, and references would be helpful to further clarify SCRM use in the Framework

RFC Response Examples:

- Furthermore, both care providers and public health leaders have great concerns with respect to the medical device supply chain, given the potentially significant risk to patient safety. Accordingly, [The Organization] recommends that the Framework provide more granular detail on the "how" and "why" of SCRM, to include a relevant context of insider threat detection and management.
- NIST has written extensively on supply chain issues, and should clearly cross reference and provide mapping to ensure that the addition of SCRM to the Framework does not confuse organizations that might look to NIST for guidance.
- To improve the usability of the CSF and the new parts on Supply Chain Risk Management, we suggest providing references to other materials, such as [The Organization] ICT Buyers Guide and resources NIST has developed (e.g., profiles for the CSF). Such resources can be used to explain how the new additions of Supply Chain Risk in CSF V1.1 are used in practice.
- The maintenance of the CSF's broad usability across a diverse set of stakeholders is key in the Framework's success and adoption in the U.S. and internationally. Additions of new topical areas, such as supply chain risk management, should reflect needs of the cybersecurity ecosystem and be done in a way that is both scalable and flexible to accommodate the differing risk management needs and resources of the highly varied set of Framework users. By focusing on processes and outcomes generally and highlighting specific standards and guidelines that explicitly and comprehensively address software and hardware integrity and supply chain security practices in the informative reference sections, users are able to select those aligned with their profiles. Subsequently, the key message that supply chain security is an integral component of cybersecurity risk management is strengthened.
- In addition to the cyber supply chain risk management activities outlined in Section 3.3 Communicating Cybersecurity Requirements with Stakeholders, when discussing global cybersecurity supply chain risk management activities, NIST may want to add identifying sovereign and regulatory risks to the list of activities. For example, users of the framework may want to consider what risks are involved in sole sourcing (when only one known source exists or that only one single supplier can fulfill the requirements). For instance, there could possibly be risks involved with critical parts from nations with hostile or unstable relations, not to mention, the difficulties with export/import licenses.
- To be useful to small businesses across various sectors, NIST should consider other steps an organization can take to improve its SCRM, providing recommendations that small business can strive for and that are realistically obtainable within the marketplace.
- However, in describing the organization-wide approach to managing cyber supply chain risk, NIST suggests that this process is likely handled within a governance structure, such as a risk council. While this may hold true for many large firms, a separate risk council likely does not exist at mid-sized and small firms. We suggest including in the example "Board of Directors or other appropriate governing body".

Representative Questions

- What types of SCRM references, examples, use cases exist today that are useful?
- What aspects are especially helpful?
- How are references, examples, and use cases used successfully in other topics related to cybersecurity?
- Does the entity diagram or process in the updated Section 3.3 encompass the SCRM function in your organization and lend itself to be used as the basis of examples?

The addition of a measurement section was deemed important by many, with further development of the measurement section recommended

RFC Response Examples:

- The measurement text is a good first step in helping to define metrics and measures although additional treatment, either within the framework proper or perhaps better in a guidance document would help step an organization through the process.
- [The organization] appreciates the potential value of mechanisms that can help organizations measure their cybersecurity risk management, but as currently written, the discussion of metrics included in the Framework update will not help [the organization's] members to measure or demonstrate cybersecurity. The discussion fails to convey clear, definitional guidance, and this lack of clarity is likely to frustrate small operators and may lead some to give up on the Framework altogether.
- [The organization] understands the subject of cybersecurity measures and metrics is a difficult one and applauds NIST's attempt at addressing it in the Guide. However, we find the treatment as written, here and in subsequent sections, may be somewhat obtuse for the average reader.
- We do not believe the Measuring and Demonstrating Cybersecurity is ready to be included. This section is confusing as to what it is trying to do. It seems to be trying to establish a language for use but does not do so in a manner that adds benefit and improves the Framework.
- Clarify the Scope and Purpose of the New Section on Measurement, and Work on Building Consensus in a Parallel Work-stream.
- [The organization] supports NIST's efforts to introduce means of applying metrics and measurements to Framework use….However, because the discussion around metrics and measurements is still evolving, [the organization] believes that NIST should make clear that Section 4.0, Measuring and Demonstrating Cybersecurity, and particularly Subsection 4.2, Types of Cybersecurity Measurement, are meant to serve as potential guidance for organizations that wish to develop measurement systems, rather than a specific recommended approach.
- [The organization] believes this is a great addition and VERY important, however it need to be more clearly explained. [The organization] would suggest taking another shot at rewriting that one.
- NIST should acknowledge these conclusions and work with industry practitioners who man the front lines to come up with an approach that aligns with the business reality. Industry is more than willing to work with NIST and other measurement experts to evolve the risk management measurement process…
- NIST should acknowledge that measurement is evolving and there is no consensus around metrics or measures.

Representative Questions:

- Is the purpose of the measurement section clear?
- Is a high-level taxonomy the best way to include cybersecurity measurement? Is it understandable?
- Is additional detail needed to clarify cybersecurity measurement? Are informative metrics (similar to Informative References) needed?
- Are the four words of that taxonomy and the relationship of those words to the components of the Cybersecurity Framework understandable?
- Where would you like to see this topic go from here?
- What specific changes to the measurement section are needed before it is ready for modification and inclusion in the update? What is the best way to further advance this topic? Who might contribute to that goal?

The measurement section should be labeled to clearly indicate that measurement provisions should be for internal or self-assessment use

RFC Response Examples:

- NIST should make clear that its inclusion of measurement is intended to support a common taxonomy for voluntary self-assessment of the effectiveness of a risk management program. NIST should re-name the section "Self-Assessment."
- The measurements and metrics should support a voluntary self-assessment approach, and not some external purpose.
- The suggested language in Section 4 may open the door to mandatory or quasi-mandatory compliance regimes. Should it become final, regulators would likely state that the audits carry an imprimatur of approval by the Framework—and so should be implemented wherever possible. Regulators may easily stop short of issuing a rule with explicit mandates and instead issue "guidance." Such guidance would inevitably become a de facto requirement; such is the importance corporate counsels attach to regulatory "guidance."
- The draft may increase security concerns due to possible public disclosure of measurement information. While risk assessments and detailed security planning are valuable, these activities are highly sensitive and, for private companies, proprietary.
- Therefore, [the organization] cautions NIST that in seeking to measure beneficial cybersecurity outcomes, private sector organizations should not be compelled to disclose these metrics to third parties, either public or private entities.
- Until a methodology for calibrating risk metrics across firms is developed and validated, metrics should be used to measure improvement by comparing a single firm's current performance to its past performance, but should not be used to compare firms with one another.
- The draft seems to indicate that the audience for cybersecurity measurements and metrics is externally focused. However, measurements and metrics should provide guidance for the internal senior management, risk managers, and the internal compliance functions.
- NIST should even more explicitly clarify that the purpose of cybersecurity measurement as contemplated in draft Version 1.1 is for organizations' internal use.
- While it's of course true that some organizations may choose to hire external third-party auditors to make such assessments, doing so may likely be cost-prohibitive for many other organizations, while others may simply prefer to conduct such assessments "in house." We recommend that NIST clarify that decisions regarding use of cybersecurity metrics and measures by organizations should remain within the sole province of organizations.

Representative Questions:

- How do you share results of assessments internally?
- How do you transform assessment information so that it can be shared outside of your organization (e.g., anonymization, aggregation, scoping)?
- How do you align and communicate organizational cybersecurity requirements, processes, and programs outside of your organization? Is measurement a part of that communication?
- How do you consume those things from other organizations? Is measurement a part of that communication?

Care should be taken to ensure continued risk-based application of the Cybersecurity Framework and to avoid compliance-based application

RFC Response Examples:

- The suggested language in Section 4 may open the door to mandatory or quasi-mandatory compliance regimes. Should it become final, regulators would likely state that the audits carry an imprimatur of approval by the Framework—and so should be implemented wherever possible. Regulators may easily stop short of issuing a rule with explicit mandates and instead issue "guidance." Such guidance would inevitably become a de facto requirement; such is the importance corporate counsels attach to regulatory "guidance."
- We are concerned the current draft's proposed approach to metrics and measurement is self-referential and may lead toward an inappropriate checklist compliance regime that is counterproductive to sustainable cybersecurity
- Furthermore, by devising structured metric and measurement parameters that can be explicitly used to support external audits and conformity assessments, NIST risks creating a perception that the CSF will lead us down a path of compliance, benchmarking, or reporting.
- Suggestion: Section 4.0 should be revised to avoid a compliance mindset that can lead to misuse.
- NIST should make clear that measurements and metrics are not tools to monitor compliance with the Framework or to comparatively assess organizations.
- An overemphasis on metrics and measurement without a clear linkage to purpose and use will result in a static, compliance-focused mindset and ultimately hinder overall culture and efforts to manage cybersecurity over time.
- To suggest that the path to better cybersecurity metrics lies through audits or compliance assessments is to set the private sector on the wrong path. The term "audit" has a long and generally well-understood meaning. The reality is that in most companies they are more afraid of the cybersecurity auditor than they are the cyber attacker.

Representative Questions:

- What components of the Framework support a risk-based approach?
- How does your organization determine "acceptable" levels of risk?
- How can organizations work with their regulators to set cybersecurity expectations and avoid regulation? What role does measurement play? What about confidence-building mechanisms like external assessments?
- What can organizations do to demonstrate confidence in Framework use?
- What are the most effective internal-assessment tools?
- What methods are most effective in tying business outcomes to cybersecurity outcomes?

Recommendations were made about categories of measurement

RFC Response Examples:

- There should be a detailed exemplar of potential metrics and measurements for the Framework in an appendix so that organizations have a starting point for implementation and can select what works for their environment.
- [The organization] suggests NIST utilize the next iteration of the Framework to explain how metrics and measures are used to assess progress with it (e.g., guidelines for using metrics and measures, use cases, etc.).
- While we appreciate the addition of this new section, NIST should consider including recognition of entities that are already subject to strong supervision and examination by regulatory bodies, such as community banks and credit unions.
- What's missing is any independent way to measure how implementation of a control (or set of controls) has reduced a company's risk exposure in a cost-effective manner.
- What companies truly need is a way, by example and case study, to observe how a control (or set of controls) diminishes risk exposure and the costs associated with that diminishment across multiple sectors for small, medium, large entities. For that, companies need a way to quantify cyber-risk and observe the effect of controls on their risk exposure.
- NIST should promote development and use of cybersecurity metrics that are designed to be outcome-oriented and aimed at supporting a company's specific performance goals and objectives
- NIST should proceed iteratively here, developing workable and reliable metrics for internal company use, before moving toward development of comparative measures.
- SP 800-55 (R1), Performance Measurement Guide for Information Security, 1 July 2008, should be incorporated into the Framework Draft. SP 800-55 (R1) assists in the development, selection and implementation of measures to be used at the information system and program levels. SP 800-55 (R1) provides a quantitative approach to measuring and analyzing security control implementation and effectiveness at the information system and program levels, aggregated across multiple individual efforts.
- Metrics should reflect and support the various strategies for all aspects of the organization, including finance, marketing, competition, standards, or customer requirements and expectations. Metrics indicate the priorities of the company and provide a window on performance, ethos and ambition.
- Include sample effectiveness measurements for each control.

Representative Question(s):

- What organizational goals and objectives should be the focus of measurements?
- What are the metrics or measurements that you currently use to track performance? How do you currently track the effectiveness of security controls? What other cybersecurity measurements are in the ecosystem?
- Is there an optimal progression for including measurement in the Cybersecurity Framework (e.g., internal company use, then comparative measures)?

Some suggested less emphasis on quantitative measurement

RFC Response Examples:

- NIST should be cautious about relying too heavily on quantifiable metrics or a "scorecard" of measures implemented. Cybersecurity is not an exact science that can be readily reduced to a quantifiable measure, and the limits of conventional quantitative metrics are exacerbated by the vast differences in risk profiles.
- Qualitative and quantitative approaches for understanding risk management posture and goals, including the measurement and metrics guidance, should be developed in supplementary documents rather than in the Framework itself.
- Rather than creating additional qualitative measurements, guidance in supplementary documents could clearly link guidance or use cases with these existing aspects of the Framework, which would encourage use of these approaches and better serve users' needs.
- Quantitative approaches are very nascent, evolving, and context dependent, so NIST should consider convening groupings of different sectors or communities of interest or work within existing partnership forums, such as the sector coordinating councils, to develop use cases for metrics and measurement that ground approaches in examples and practical application.
- NIST should employ an outcome-oriented Risk Management approach to cybersecurity metrics in lieu of over-reliance on conventional quantitative measures.

Representative Questions:

- Does your organization rely on qualitative, quantitative, or both types of measures for cybersecurity risk management?
- What is the relative value of qualitative and quantitative measures?
- Is there a difference in the level of maturity and research of qualitative versus quantitative measurements?
- Are there distinct use cases for qualitative versus quantitative measurements?

Respondents affirmed the integration of SCRM into the Core. Some respondents suggested SCRM be integrated across existing Categories, rather than adding an SCRM Category to the Identify Function

RFC Response Examples:

- As stated above, the additional discussion of SCRM is the most impactful change for [organization] members.
- We view the addition of supply-chain risk management as a substantial improvement to the original Cybersecurity Framework, provided that it aligns with the aforementioned NERC CIP013-1.
- Regarding the addition of the "Supply Chain Risk Management" Category, [the organization] welcomes this addition. It is an appropriate progression of the Framework and it integrates an essential component to any thoughtful cyber risk management program.
- With continued cyber breaches often resulting from poor supply chain management, emphasizing SCRM controls is very important. While NIST 800-161 succeeded as an interim reference document, we have found organizations using supply chain controls as a side project. It has been proven time and time again that organizations are only as secure as their weakest link. Now that SCRM controls are integrated into the NIST CSF, we expect to see the controls being more widely adopted in commercial industries. These controls are an excellent step toward codifying the genetic structure of cyber supply chain risk.
- Integrating Supply Chain Risk Management into the Framework is Timely, but Must be Done Carefully. Addressing global supply chain security concerns has long been a priority for [the organization] and our members. While [the organization] has noted in previous public comments to NIST that some [organization] members had begun exploring how to expand Framework use with their suppliers, we cautioned against prematurely incorporating SCRM into the Framework Core at its inception, given the lack of consensus-based industry-led international standards in the SCRM area at the time.
- As a general matter, [the organization] is hopeful that the changes in draft Version 1.1, if adopted, can have a positive impact on the cybersecurity ecosystem by addressing two increasingly important issues – metrics and supply chain risk management ("SCRM")
- Regarding the architecture of the Core, all new SCRM processes were added in one place — Supply Chain Risk Management (ID.SC) — opposed to integration based on the primary activity required to implement the control. For example, the primary activity to implement the following control is response and recovery planning: "ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers." The usability of the Framework would be lessened by forgoing a control activity based implementation taxonomy that is used for the current, non-SCRM subcategories. We believe that these revisions will help Framework users implement cybersecurity controls and achieve results outlined in the "Subcategory" section, thereby improving the cybersecurity posture of the organization.
- In draft version 1.1 there is an entirely new Category (ID.SC) added under the Identify Function. This seems extremely limiting. Not all cyber SCRM activities will or should reside in just one function. We believe SCRM-related concepts and activities should be incorporated across the Functions, into existing Categories, creating new subcategories where relevant and appropriate. As with items such as cyber threat, information sharing, vulnerability disclosure, and other areas, SCRM references, such as SP 800-161 and SP 800-53, should be added to the appropriate and relevant subcategory Informative References.
- Over the past few years, significant work has been done to mature SCRM standards and best practices, thus the inclusion of SCRM at this stage in the Framework's evolution seems both appropriate and timely. However, we recommend simplifying the SCRM language in draft Version 1.1 and integrating it within all relevant Subcategories and Informative References in the Core, rather than including such

guidance in the Tiers.

- There is an argument that by including supply chain risk at the Category level in the Identify Function it promotes awareness of the importance of addressing supply chain risk as part of the CSF risk analytic model, but doesn't complicate the use of the CSF by interjecting it at a similar level of other Functions. But will including it in the Identify Function suggest that there is no connection between supply chain risk and the Functions of Detect, Protect, Respond, and Recover?
- It is not clear that it is the right decision to add supply chain risk ONLY to the Identify Function and not in one or more other Functions, such as Detect and Protect. But it is not a clear matter.
- Supply chain risk management should be integrated throughout the Core's Subcategories and Informative References rather than within the Implementation Tiers. Inclusion of supply chain security, a topical area, creates confusion about how to use of the Tiers; integration of supply chain security across relevant areas of the Core, however, more effectively incorporates all the organizational stakeholders whose responsibilities may contribute to overall supply chain security.
- …we strongly urge NIST not to incorporate Supply Chain as its own new Category. Supply Chain is a valid lens (context) through which to look for risk, but such cybersecurity risks should be woven into the Framework.
- …[the organization] urges NIST to incorporate relevant SCRM concepts into existing Categories, creating new subcategories where and if necessary.
- Additionally, although the updated Framework adds a new category for SCRM (under the umbrella of the "Identify" Function), there is neither a subcategory nor corresponding informative references that relate specifically to buying decisions.

Representative Questions:

- Should SCRM be integrated into the Framework Core through the proposed 23rd Category (under Identify), through the pre-existing 22 Categories, both, or via another approach?
- Would applying SCRM to the 22 existing categories necessitate changes to those Categories? If so, what changes? Would this approach uphold the concept of "backwards compatibility" with Vresion 1.0?

Respondents affirmed the enhancement of the Identity Management, Authentication and Access Control Category and provided further thoughts for consideration

RFC Response Examples:

- The addition of authentication and identity proofing to the previously named Access Control category brings this section more in line with the Identity and Access Management programs, which most companies have.
- The proliferation of IoT devices and the increasing adoption of "bring your own device" policies have made identity management and device authentication mechanisms a critical element of network security for enterprises of all sizes. The addition of guidance on Identity Management and Authentication to the pre-existing Access Control category in the Framework Core will help organizations better manage potential endpoint security risks associated with these developments.
- To stay consistent with the CIA Triad, I agree with the decision to include authentication and authorization under the Access Control Category, and create a subcategory that accounts for identity proofing
- Authentication must be explicitly addressed in updates to the Framework Core. If the Framework is to meet its goal of helping critical infrastructure entities across both government and industry better manage cyber risk, then the risk caused by inadequate authentication mechanisms must specifically be addressed in the Framework core. No other cyber-attack vector has been exploited as much in the three years since the CSF was published.
- The refinements to better account for authentication, authorization, and identity proofing more accurately reflect the state of the art in identity and access management best practices, which will have a positive impact on the cybersecurity ecosystem. (p. 32).
- Strengthening authentication & identity management in the Framework Core: We were pleased to see movement on the Authentication Roadmap Item, but were surprised to see that a critical security control such as Multifactor Authentication (MFA) was left out. MFA is a proven technology that addresses a major threat vector and at minimum should be presented as a specific option for CSF consumers. We recommend including a specific control to address MFA in the PR.AC section of the Framework.
- If multifactor authentication is to be a component of the framework, it should be expressly stated. It is not. Perhaps intentionally? Using the term "credentials" is generic and organizations will likely implement the minimum (static passwords) authentication thinking they are adhering to the framework.
- We strongly urge NIST to add a new PR.AC Subcategory for Authentication, reading: "Authentication of authorized users is protected by multiple factors."
- While the primary focus of our comments is authentication, we are highly supportive of other identity-centric changes to the PR.AC function, including: The addition of a new control – PR.AC-6 – focusing on ensuring that "Identities are proofed and bound to credentials, and asserted in interactions where appropriate."
- Add a subcategory on "Privileged User" under the "Identity Management and Access Control" function.

Representative Questions:

- Are the enhancements made to the Access Control Category enough to ensure the breadth of Identity and Access Management is addressed? If not, what additional enhancements do you recommend?
- Given the Cybersecurity Framework precedent of not specifying baseline configurations (i.e., not specifying "how much" cybersecurity), should concepts like multi-factor authentication be referenced in the Cybersecurity Framework? If so, how?

Modifying and improving the usefulness of Informative References is appropriate, and the process for determining future Informative References should be defined

RFC Response Examples:

- I would request that the Information Security Form Standard of Good Practice be included in the next release of the CSF.
- I was under the impression that the first revision of the CSF would include references to the Information Security Forum (ISF) Standard of Good Practice (SoGP), but that doesn't seem to be the case. We and other large organizations rely on the SoGP, and the ISF has itself produced a very detailed mapping. I would like to see it included, please. This might seem a trivial point, but it is not. The CSF has seen remarkable buy-in at senior leadership levels across industries, and by not including a major, comprehensive standard, it forces security practitioners who rely on the SoGP to accommodate other standards that might not be best suited for the organizations.
- Location: Line 654 Rationale: It seems that although this section alludes to the fact that there is the opportunity to identify additional Informative References, there is in fact no defined path to do that. After participating for years in the NIST CSF workshops, advocating the need for referencing existing supply chain security standards and best practices, there are still no informative references for supply chain standards, even in this new revision where supply chain is now addressed. Comment: This section states the following: "The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices." While this explains how you can address gaps it doesn't provide a path or describe the method that is used to get an existing standard included as an informative reference. If there is a path for that process (other than submitting comments to the RFC) it would be helpful to understand what that is, including the decision process for accepting an informative reference.
- Page 25, lines 864-866. The [organization's] CSF is one of the most widely adopted security controls frameworks in the industry. Given that healthcare is said to be as much as 1/5th of the U.S. economy and the [organization's] CSF is extensible beyond the healthcare industry (as demonstrated by its application to business associated that also serves other industries, e.g., Cloud service providers), [The organization's] CSF controls should be included in the NIST Cybersecurity Framework Core's Informative References.
- Finally, because a new category has been proposed to be added to the Identity Function for supply chain risk (Supply Chain Risk Management (ID.SC)), along with several sub-categories within that category (ID.SC1-ID.SC5), I recommend that the informative references that were added for these new subcategories be further revised to add relevant supply chain security standards.
- The Informative References column in the Framework Core needs to include references to the relevant topics as covered in the ISF Standard. This will help us to demonstrate how these two standards are aligned (e.g. to executive management, operations staff and suppliers).
- Continuous improvement to update Informative References and relevant Categories and Subcategories. [The organization] encourages NIST to continue to revise the Cybersecurity Framework Core with updated Informative References and relevant categories and subcategories. One example would be including a new category of "Using Threat Intelligence" under the "Detect" function; sub-categories would include "Automated Indicator Sharing" and "Data Analytics". As virtually all critical infrastructure sectors have at least one Information Sharing and Analysis Center (ISAC) and with the growing acceptance of the STIX/TAXII information sharing specifications, API feels this category is sufficiently defined to be included in the framework core.

- NIST can promote broader adoption of the CSF by more explicitly encouraging organizations to integrate other third party-validated certifications and attestations that achieve equivalent security outcomes yet are not specified in the Informative References. Often times, CSF consumers view the Information References as an exclusive, authoritative list of acceptable certifications without realizing that it was not intended to be comprehensive, but rather illustrative and suggestive. Recommendation: By clarifying that CSF adopters have the discretion to leverage other industry accepted certifications, attestations, and models as Informative References, NIST can increase the value proposition, scale, and use of the CSF.
- I'd like to suggest that the informative references section of the core Excel docs include references to 800-171, if possible. I understand that cross-correlation is providing within 800-171—but the smaller businesses that seek compliance with this document can be aided by the framework references.
- In particular, we suggest adding the following to the informative reference sections in ID.SC: ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders o ISO/IEC 20243 4.1 – 4.2.1.12
- In particular, we suggest adding the following to the informative reference sections in ID.SC: ID.SC-2: Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process o ISO/IEC 20243 4.1 – 4.2.1.12, Assessment Procedures for 20243 4.11- 4.22
- ID.AM-1: Add PCI DSS v3.2 2.4, 9.9, 11.1.1
- ID.AM-2: Add PCI DSS v3.2 2.4
- ID.AM-6: Add PCI DSS v3.2 12.4, 12.5, 12.8, 12.9
- ID.GV-1: Add PCI DSS v3.2 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1
- PR.IP-1 has the incorrect reference to CCS CSC 10 (Data Recovery Capability), when it should reference CIS CSC 9 (Limitation and Control of Network Ports, Protocols, and Service) and CIS CSC 11 (Secure Configuration of Network Devices).
- PR.IP-2 should reference the CIS CSC 18 (Application Software Security)
- PR.AT-1 through 5 have the incorrect reference to CCS CSC 9 (Limitation and Control of Network Ports, Protocols, and Service), when they should reference CIS CSC 17 (Security Skills Assessment and Appropriate Training)
- PR.DS-1,2,5 have the incorrect reference to CCS CSC 17 (Security Skills Assessment and Appropriate Training), when they should reference CIS CSC 13 (Data Protection)

Representative Questions:

- How should NIST balance readability of the Cybersecurity Framework with comprehensiveness of the Informative References?
- Should the update cycle of Informative References drive an update cycle for the Cybersecurity Framework, or can Informative References be revised without revising the entire Framework?
- What should the criteria be for including a reference as an Informative Reference?
- What process should be used to identify, adjudicate, and integrate references as Informative References? What other initiatives use similar processes?
- Are technologies such as the CSF Reference Tool helpful in viewing and processing Informative References?
- What references are missing that should be considered? Small and medium business references? International references?

NIST should continue to support Small Business involvement with the Framework and provide greater clarity about how smaller businesses can use the Framework

RFC Response Examples:

- We also encourage NIST to support legislative and executive branch policies that would support its capacity to engage more directly with the small business community.
- NIST should partner with the Department of Homeland Security ("DHS"), Department of Commerce ("DOC") and/or the Small Business Administration ("SBA") to develop a comprehensive Small Business Cyber Program. The Program should endeavor to aid small businesses in their use of the Framework, by first determining what gaps might persist in cyber practices, and then what practices (aka "incentives") might be helpful to address those gaps.
- Small businesses need a prioritized set of cybersecurity controls. As helpful as the Framework is on an operational level, it was largely designed by and for larger companies. Its multiple tiers and ninety-plus subcategories make it unsuitable for the clear majority of small companies. This is not to say the Framework can't be used by smaller companies (some do). However, the multiple assessments smaller firms would have to undertake to locate what parts of the framework offer the most cost effective way to spend their next marginal dollar on cybersecurity is too great a burden for small firms operating on thin margins.
- [The organization] supports Framework Version 1.1 guidance for small- and medium-sized businesses: We recognize the importance of accessible and practical risk management frameworks and related support for smaller businesses. Cybersecurity threats and vulnerabilities affect businesses of all sizes. We encourage NIST to continue developing the Framework and complementary guidance and resources to ensure that our small business community has appropriate guidance and resources to be a full partner in cybersecurity risk management.
- To be useful to small businesses across various sectors, NIST should consider other steps an organization can take to improve its SCRM, providing recommendations that small business can strive for and that are realistically obtainable within the marketplace.
- This discussion suffers once again from a lack of clarity that makes it less useful to smaller entities. For example, the Framework states that, in situations where the organization cannot impose a set of requirements on its supplier, its objective "is to make the best buying decision, optimally between multiple suppliers, given a pre-decided list of cybersecurity requirements." Unfortunately, the discussion provides no insight into how a small entity might evaluate whether a potential vendor meets their cybersecurity requirements.

Representative Questions:

- Are there any updates that can be made to the Framework that can accelerate and improve SMB use or reduce confusion?
- Should SMB-specific guidance be considered to help SMBs to adopt cybersecurity risk management? If so, what are the best formats for these documents? What is the best way to share them?
- What are examples of SMB-specific incentives to use cybersecurity risk management?
- What are challenges unique to SMB cybersecurity risk management that can be addressed in the Framework ecosystem?

Continue to promote the Framework internationally in the interest of alignment and common approach

RFC Response Examples:

- [The organization] encourages NIST to continue global outreach programs to help align cybersecurity regulations or requirements across the world to the CSF. The common taxonomy and method of the CSF benefits multi-national [organization] members who can use common processes to address cybersecurity issues rather than having to devote scarce resources to managing different nuances of different regimes across the world.
- To facilitate further global adoption, NIST and its Federal agency partners should continue to promote the Framework approach with their global government partners, and NIST should make some reference to these efforts in draft Version 1.1.
- [The organization] previously advocated that global policymakers also stand to benefit from becoming more conversant in the language of the Framework, and cautioned against making drastic changes to the Framework core, as doing so would be the equivalent of scrambling the Framework's alphabet at the same time many are still trying to learn or master the language. On balance, NIST has recognized the need to tread lightly with respect to draft Version 1.1, with an eye toward refinement to make the Framework a more valuable tool to a broader array of organizations, rather than offering a significant expansion that may chill its uptake.
- NIST should also consider other mechanisms by which to expand the Framework approach. For example, given the increasing global acceptance of the Framework, we would support NIST exploring, with industry stakeholders, the opportunity for submitting relevant parts of the Framework as an international standard. This could be a valuable contribution to further harmonizing cybersecurity practices on a global scale.
- There is not only an opportunity for but rather a need for the U.S. Government to promote the Framework, the approach used to develop it, and the attributes that make it effective—both domestically and internationally.
- Increased promotion of the Framework. To strengthen common foundation introduced by the Framework, it should be offered and promoted internationally as well as domestically. It should be actively shared with international governments, standards organizations, and industry sectors.
- NIST and its federal agency partners should increase resources dedicated to the promotion of the Framework, and its flexible, technology-neutral approach with global government counterparts. International acceptance of industry-led, global cybersecurity standards allows for even greater competition and innovation in the marketplace. International adoption of the Framework approach to critical infrastructure cybersecurity establishes a common lexicon across a range of stakeholders, yet allows for technology flexibility to address unique threats and priorities.

Representative Questions:

- What other nations and non-U.S. industries currently use Cybersecurity Framework? What actions did those nations take to facilitate use? What customizations were needed to ensure use by other nations? Should those customizations be included in version 1.1?
- Would international standardization through standards development organizations (e.g., ISO, IEC, ITU) sufficiently catalyze use in various nations and national industries?
- What engagement models do you recommend to NIST to maximize use and alignment internationally?
- Would the proposed updates to the Framework help or hurt international alignment?