Analysis of Cybersecurity Framework RFI Responses

Applied Cybersecurity Division, Information Technology Laboratory
National Institute of Standards and Technology (NIST)
March 24, 2016

1. Introduction

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636[1], Improving Critical Infrastructure Cybersecurity, in February 2013. The order directed the National Institute of Standards and Technology (NIST) to work with stakeholders to create a framework – based on existing standards, guidelines, and practices – to provide a repeatable, flexible, and cost-effective means for critical infrastructure to identify, assess, and manage cybersecurity risk. As the result of this collaborative process, NIST published the Cybersecurity Framework[2] (Framework) in February 2014.

The Cybersecurity Enhancement Act of 2014 (CEA, Public Law 113-274) reaffirmed NIST's involvement and approach. CEA calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. NIST continues to collaborate with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework. On December 11, 2015, NIST issued its third Request for Information (RFI)[3] to receive feedback on the Framework. This document provides analysis of those responses.

This analysis represents an initial, high-level evaluation of the RFI responses NIST received. The analysis will serve as a starting point for discussions at Cybersecurity Framework Workshop 2016[4]. Stakeholders are asked to evaluate the themes identified by NIST, determine if these themes are reflective of the comments received through the RFI, and assist in those areas where additional stakeholder engagement will be needed to guide the Framework and the Framework program.

2. Analysis Methodology

NIST implemented a consistent and repeatable methodology to conduct its analysis of the 105 RFI responses[5] to the Federal Register Notice 80 FR 76934[6]. Each RFI response was reviewed and analyzed by NIST according to the following process:

---

[1] [LINK] https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity
[2] [PDF] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[3] [LINK] https://www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity
[4] [LINK] http://www.nist.gov/itl/acd/cybersecurity-framework-workshop-2016.cfm
[5] [LINK] http://csrc.nist.gov/cyberframework/rfi_comments_02_09_16.html

- Determine basic respondent information, including sector, size, and organization type;
- Identify sections of text relevant to one or more of the RFI questions;
- Specify terms and phrases that identify key points in each section of relevant text ("Associated Key Terms/Phrases").

To identify RFI response themes, the key terms/phrases were then used to identify commonalities and recurring language. Respondent quotes ("RFI Response Examples") were then associated with themes. Finally, NIST augmented each theme with Representative Questions that will serve as a starting point for discussions at Cybersecurity Framework Workshop 2016.

Multiple teams evaluated RFI responses according to the above process to arrive at independent conclusions. Those independent conclusions were compared to ensure parity. That refined analysis is shown below.

3. Themes from RFI Analysis

A theme is the observation of commonality or dissonance across many RFI responses. Analysts sought out themes regarding answers to RFI questions. Sometimes, themes emerged from RFI responses, but not necessarily in response to a specific question. A summary of RFI response themes and subthemes is listed below.

- Framework Update Timeline – There were diverse comments on whether an update is necessary or desirable.
- Update to Framework Content – Many respondents had specific suggestions of ways to update and expand the Framework.
- Update Process – The Framework should be updated through a collaborative process and with minimal disruption to current industry use.
- Framework Governance – Respondents are comfortable with NIST's continued leadership in the Framework process, though transition should be considered at a later date.
- Optimal Industry Leadership – Any possible future steward of the Framework should be a respected, internationally recognized, neutral, 3rd party organization.
- Industry Resources - Industry resources are useful but additional guidance is needed, especially for small and medium-sized businesses.
- Challenges in Sharing Best Practices – There is a need for additional sharing of best practices surrounding use of the Framework
- Regulation – Many users of the Framework say that regulation is a necessary consideration in the development of their cybersecurity programs and caution about the potential negative impact of additional regulatory requirements.
- International Alignment – The Framework is gaining traction internationally, but still needs continued outreach.
- Awareness – Much progress has been made in spreading Framework awareness, but more is still needed.

[6] [LINK] https://www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity

a. Themes in a Potential Framework Update

Framework Update Timeline

There were diverse comments on whether an update is necessary or desirable.

Associated Key Terms/Phrases:

- Update Now
- Do Not Update
- Living Document
- Recurring Updates
- Update as Industry Evolves

RFI Response Examples:

- In the short and intermediate term, perhaps it is best to not change the framework, but instead focus on making it easier to understand and incrementally implement. The framework is valuable as is, and while maybe not perfect, can help get industry on the road to higher security.
- If any changes are made, they should not be more frequent than annual (at most), and they should be published in parallel with a guide to what the changes were and tips on how to migrate the delta to the new guidance.
- It should be a living document that keeps pace with the evolving cybersecurity environment and new technology uses such as Internet of Things and the proliferation of Bring Your Own Device.
- The framework should be updated on periodic basis. This would allow new or outdated information to be incorporated (e.g. regulatory changes and leading practices).
- The framework should be continuously reviewed and updated.
- Yes, the Framework should be updated. To further capitalize on progress in the Framework's implementation, [the organization] recommends that the Framework be updated on a regular basis to reflect state-of-the-art risk management best practices which are constantly evolving. This will help organizations reduce the frequency, severity, and impact of attacks as cyber threats evolve their tactics and techniques.
- The framework should continue to evolve as existing standards are updated, and new standards are released.
- Just as we continually update our profile documentation, the framework should be updated to stay current with trends as well as responsive to feedback from the critical sectors.
- The Framework should reflect "current best practices", but an update should not be undertaken at this time. The Framework is more than sufficient to enable its intended results in its version 1 form. While there are some enhancements that should be made, they are not of sufficient magnitude or value to warrant the effort expended to produce an update at this time.
- The [organization] observes that Version 1.0 of the Framework has not yet reached full maturity, which moderates the call for large-scale revision. Rather, NIST might consider a Version 1.1, revising individual items described in the companion Roadmap and selected target areas for an iterative update.

Representative Questions

- Should updates occur on a recurring basis or only 'as needed'?
- What industry developments would act as a trigger for 'as needed' updates?
- Should Informative References be updated more regularly than other parts of the Framework, and do they need to be reviewed by a public comments mechanism? If so, should the Framework document be updated with every change in Informative References?

Updates to Framework Content

Many participants suggested updating and expanding the Framework.

Associated Key Terms/Phrases:

- Expanded Functions
- Updated Informative References
- Expanded Subcategories
- Tier Usability

RFI Response Examples:

- [The organization] recommends adding a section to the Framework document that specifically addresses how small, less mature organizations can implement the framework consistent with the recommendations outlined in NISTIR 7621, Small Business Information Security: The Fundamentals.
- Add Threat Intelligence as a Category under the Detect Function. It's not the same as event detection and, especially with the growth of ISACs, the NCCIC, etc., it needs its own area. The Respond and Recover Functions need some more filling out. Especially Recover, which is often not part of or well integrated with enterprise Cyber Security activities. Lastly, it really needs a more visible Governance section. Either a 6th Function or a Category under Identify. Too much of the governance (policies, RAA, etc.) are scattered in the Sub-Categories – which are not very visible.
- The implementation tiers should be changed in such a way that they relate to the core profile work that is to be completed. As it currently stands, they are a standalone piece; however, we think there is value in applying the implementation tiers to the core."
- [The organization] supports the inclusion of additional informative references that help organizations achieve the security outcomes in the Framework subcategories, if they have broad support and are underpinned by global, industry-driven standards.
- Add:
  - Expanded Subcategories, best practices, for Threat Intelligence and information sharing.
  - How to "implement" or "operationalize" the Framework supporting materials (see specific suggestions below).
  - Measurement and Metrics guidance and recommendations.
- Maturity Models. As is discussed later in the document, several of our members agreed that while NIST notes that the framework is not a "maturity" framework that is actually how providers tend to use it. We believe this should be remedied and adopted as a maturity model so that providers have a common lexicon for benchmarking themselves amongst one another.
- Because there is not a developed methodology for how to calculate and apply Tiers, using the Tiers outside of an organization's risk management process runs the risk of false comparisons between organizations based on non-standard profiles.
- Any movement beyond the Privacy Methodology set forth in Version 1.0 runs the risk of layering an additional and unnecessary set of privacy obligations on top of the existing frameworks that our members already adhere to, thereby imposing more complexity, cost and compliance burdens, with little incremental improvement to privacy or cybersecurity.
- … the healthcare sector could benefit from a common set of consensus-based, industry-led guidelines, best practices, methodologies, procedures, and processes in relation to privacy and information security risk management. Thus, the Framework could be greatly enhanced in this area.
- The Framework would benefit from expanded supply chain management content and practices to more systematically address managing those risks across the lifecycle of relationships with external entities/suppliers.
- We suggest the addition of a new PR.AC Subcategory around Authentication, reading "Authentication of authorized users is protected by multiple factors."

Representative Questions:

- What topics should be introduced / expanded upon in the Framework Core?
- Should the Respond and Recover Functions be expanded? If so, how?
- Should the Implementation Tiers be modified, clarified, or both?
- Should a maturity model be included in Framework?
- What industry standards / best practices should be added to the informative references?
- What supply chain risk management practices are universal enough to be included in Framework?
- Is authentication represented adequately in the Framework Core? If not, how should the core be updated?
- What role should research and development play in shaping Framework? Is there a milestone in the technology lifecycle that triggers inclusion in Framework?

Update Process

The Framework should be updated through a collaborative process and with minimal disruption to current industry use.

Associated Key Terms/Phrases:

- Enhancements vs Overhaul
- Collaborative Process
- Periodic Updates
- Living Document

RFI Response Examples:

- Suggested changes should go through a change management process, approved with an RFI published to get comments. Once finalized, there should be a "transition" window (1 - 2 years for example) to allow organizations to evaluate the changes and impact and then justify the inclusion or exclusion of the additional/updated controls.
- Today the Core is a part of the actual versioned document. If the Core was published as a separate but required document, then both the Framework Core could be extended with new Informative Reference and Categories without changing the process document.
- Socialization of anticipated Framework updates well in advance should minimize disruption and support planning and decision making for current users"
- [The organization] recommends that NIST continue to work with sector-specific agencies and independent regulators in developing sector-specific use cases and implementation guidance for the Framework.
- The method NIST used to engage with the public during the development of the Framework in 201[3] set the standard for future iterations of Framework updates. We hope NIST repeats this effort by issuing public drafts, seeking comments, and hosting stakeholder workshops for future iterations of the Framework. This transparent method, which has been effectively used by COSO and similar organizations, will improve the adoption of changes and minimize disruption for those currently using the Framework.
- Updating on an ongoing basis the Framework's Informative References will not impact use. With a publicly shared update cadence, stakeholders can also accommodate cycles of updates to other portions of the Framework.
- A change history document should be created along with a plan for how the new additions to the framework should impact and modify work that has already been done by organizations using the framework.
- Rather, NIST might consider a Version 1.1, revising individual items described in the companion Roadmap and selected target areas for an iterative update. A limited revision would enable firms to continue assimilating the current Framework without fear that their cybersecurity programs would need a near-term reengineering to accommodate a new Cybersecurity Framework. Following a Version 1.1, NIST could schedule biennial updates alternating between major and minor revisions every two years. A scheduled approach enables the Framework to be ingrained within individual firms and across sectors while evolving in response to the dynamic nature of cybersecurity risk management.

Representative Questions:

- Should the current Framework update approach be followed in the future (i.e., RFI-Workshop-public draft)?
- What steps should be taken to ease transition to future updates?
- What constitutes a major versus a minor change to the Framework? Should the implementation of major and minor versions be different?

b. Themes in Framework Governance

Framework Governance

Respondents are comfortable with NIST's continued leadership in the Framework process, though transition should be considered at a later date.

Associated Key Terms/Phrases:

- Private Sector Involvement
- Premature to Transition
- Private / Public Cooperation
- No Cost
- NIST Retention
- Open/Transparent Processes

RFI Response Examples:

- [The organization's] members urge NIST to continue to play a key role in facilitating further Framework development activities. Given the competence demonstrated throughout the effort and the proven ability to bring a broad array of stakeholders to the table, it would be premature at this time to transfer responsibilities to the private sector.
- Up until this point, NIST's oversight and has been extremely collaborative with the public sector. So much so that other Federal groups are trying to replicate the developmental model for their projects. There are some that feel future Framework advancements needs to be done outside of NIST in a private sector organization. We believe it is really too early to decide this.
- Our organization believes that the private sector should eventually govern the framework, but NIST needs to keep one hand on the wheel. NIST must maintain a key role in collaborating with industry and engaging foreign organizations and governments.
- NIST should not transition any portion of the Framework coordination to another organization at this time... Transitioning any pieces of the Framework to another organization may result in negative impacts such as limiting access of some private sector organizations to the collaborative process that created the Framework in the first place. We believe that NIST should continue to be the custodian and developer of this Framework for the foreseeable future.
- We believe it would be acceptable to consider use a 3rd party to assist in updating the framework or transitioning the document in whole. However, we recommend NIST remain involved and that more discussion is needed prior to this occurring. At a minimum if this work is moved outside of NIST it must be done in a manner that has balanced industry representation. And, we strongly recommend against transitioning to a for-profit entity or a not-for-profit entity lacking strong governmental oversight.
- NIST is well-placed in this role also because many organizations use other NIST standards and/or publications internally. There is some fear that if NIST transitioned some or all of the Framework elsewhere, the new organization may not as actively gather private input or the Framework may become a purchase-only document which would defeat the purpose.
- Ultimately, much of the governance of the Framework should transition from NIST to an international standards organization, though NIST should also continue to maintain a role in guiding U.S. organizations as they implement the Framework. Over the long term, an organization such as the International Standardization Organization (ISO) is well positioned to manage portions of the

Framework.

Representative Questions:

- If NIST continued to play an active role with the Framework, would industry, academia, and government be comfortable with other parties' involvement in the management and evolution of the Framework?
- When should NIST consider involving other parties? Is that involvement based on circumstance, or is there a logical on-going role for another party?
- What measures could be taken to minimize any disadvantages to a multi-party ownership of Framework?

Optimal Industry Leadership

Any possible future steward of the Framework should be a respected, internationally-recognized, neutral, 3rd party organization.

Associated Key Terms/Phrases:

- Not for Profit
- Transparent
- International
- Standards
- Neutral
- High-regard

RFI Response Examples:

- While there are many factors, which could be used to evaluate such capacity, ideally the partner should have an awareness of the unique challenges of the healthcare sector to reduce cyber risk, in addition to an in-depth understanding. Moreover, the transition partner ensures that cost is not a barrier to participation—ideally, the partner should not assess any cost for organizations, including healthcare organizations, to assist with development of or to use the Framework.
- [The organization] would prefer that NIST retain responsibility for the Framework but if it is decided to transition it, the Framework should be transitioned to an organization that is funded by the government or is in academia. For instance, CMMI is a solid program and many organizations are working diligently to get their CMMI certification. This is administered by Carnegie Mellon but was born out of a consortium of government and industry prior to being turned over to Carnegie Mellon. This type of cybersecurity "certification" (Level 1 - 5) would help to promote Framework adoption.
- Track record of the entity or its members (if it has members) in providing governance capability across segments. An organization which will continue to offer the NIST benefits including:
  - Transparency of process
  - Low barriers to entry
  - Ease with which to contribute / partner
  - Low/no cost to participate
  - International appeal
- Qualification factors to verify their capacity may include technical understanding of the Framework, approach to domestic/international organizations collaboration, Strategic Planning which includes goals/objects, vision, etc. to sustain the program.
- Has the organization any true experience with successful, highly collaborative efforts?
  - Is the target organization a non-profit where conflicts of interest are not possible or perceived to be possible? Does it have some direct linkage to a for-profit company? If so, is there any conflict of interest here?
  - Does the organization currently have the respect and 'brand' that would encourage active participation of the private sector going forward?
  - Is the organization currently recognized globally?
  - Does the organization have the funding and continuing revenue stream to be successful long term?
  - Will the organization be able to do national and global outreach to continue to attract use and participation in improving the Framework?
  - Does the organization have experience in cybersecurity and risk management related areas?
  - Is the organization a recent startup focused on governance of the Framework?
  - Does the organization have existing ties to international standards bodies to assure the alignment with other efforts?
- The following factors should be considered:

  - 1) The entity should be standards-based with experience in keeping a standard up to date and facilities and infrastructure to collect feedback in real time on the standards and deliver real time updates.
  - 2) The entity should have a global footprint so it can factor in foreign attacks and translate and disseminate information for the U.S. as well as share our best practices with our global allies.
  - 3) The entity should have access to FBI InfraGard, the Department of Homeland Security, the National Security Agency and other government entities who have access to information to improve the framework against changing global attack vectors.
  - 4) The entity should have background in financial security as well as general infrastructure security.
  - 5) Continued development of tools should be available to the private sector to promote the framework. The entity should foster this within the security community.
  - 6) The entity should also evolve into a source of data that is required to be implemented by organizations deemed critical to the U.S. infrastructure. This would include but not be limited to: a. A federated internet protocol (IP) black list b. A federated attack vector signature list c. Any direct threats to credit unions that are discovered by the U.S. regardless.
  - 7) The entity should be able to cross-reference global infrastructure attacks and provide predictions on known criminal or state sponsored activity.
  - 8) The entity should work with security vendors to improve the position of the framework and core by holding workshops for the vendors and including them in discussions of changes to the framework.
  - 9) The entity should improve audit guidelines and provide certification for audit firms to guarantee consistency of audits across the country as it relates to implementing the framework. This can serve as a means of income for the entity.
  - 10) The entity should work with the major data centers and carriers to help monitor threats and help coordinate defenses in terms of updating regulation in light of either past attacks or pending attacks of how credible the threat is.
- A future Framework governance organization should have the following attributes:
  - 1) international mandate and global recognition and respect as a subject matter expert;
  - 2) ability to support various implementation approaches and activities across the ecosystem;
  - 3) expertise across multiple sectors;
  - 4) demonstrated objectivity;
  - 5) unwavering commitment to engaging a broad stakeholder community, including the private sector; and
  - 6) dedicated, professional staff with technical risk management capabilities.
- Yes. It should be transitioned to a group hosted by an entity which focuses on technology concepts on a more granular level—possibly the National Cybersecurity Center of Excellence (NCCoE) or the Critical Infrastructure Partnership Advisory Council (CIPAC). The group should include the CISR R&D participants, the Sector Information Sharing and Analysis Centers (ISACs), and others interested in technological pathways to real cyber security.
- The Framework could be transitioned to a not-for-profit, U.S.-based organization with multinational private-sector representation. Participation could also be voluntary, both at an individual or organizational-level. However, nominal membership fees could be charged for both types of members, with the fees for organizations structured on a tiered model, e.g., by annual revenue. Such fees could be used to make the not-for-profit self-sustaining. The not- for-profit would only be required to hold the intellectual property and provide administrative support, similar to that provided by ISO or ANSI. (In fact, ANSI itself may be a good candidate.)
- All of these have problems. A non-profit will have to determine some means of funding continuing

updates to the Framework. A for-profit will need to make money on the venture. Each of these implies that the Framework may need to be purchased in the future, which will limit use (smaller firms may not want or could not afford to buy initial versions and periodic updates) and could then put critical infrastructure at increased risk. Multinational organizations would be better for global companies as these might have a better chance of getting more adoption of the Framework across the world. Standards organizations tend to have relatively long development and approval time frames (ISO is about five years) because of the complexity of creating and reaching consensus on updates, and this may lessen the value of the Framework due to the fast-evolving nature of cybersecurity.

Representative Questions:

- Would a consortium/group or individual organization be best suited for this role?
- Must a potential future steward be a non-profit organization?
- Are there other attributes a third party steward of the Framework should possess?
- Are there organizations that exemplify these characteristics?
- What fiscal model is best suited to sustain industry leadership?

c. Themes in Best Practice Sharing

Industry Resources

Industry resources are useful but additional guidance is needed especially for small- and medium-sized businesses (SMBs).

Associated Key Terms/Phrases:

- Awareness
- Implementation
- Training
- Forum
- Use Cases/ Case Studies
- SMB

RFI Response Examples:

- We would like NIST to focus on resources pertaining to awareness of the Framework, and practical/effective implementation of the Framework at this time.
- Collecting and making available a variety of case studies and sector-implementation approaches for implementing the Framework is useful to the organizations using the Framework. For example, C2M2 is widely used by electric utilities because it helps gauge maturity of security programs along 10 functional domains. Using C2M2 in conjunction with the NIST Framework is detailed in the Energy Sector's NIST Cybersecurity Framework Implementation Guidance. However, such case studies need to be carefully organized and categorized to avoid overwhelming the audience with the content and the detail that is not relevant to them. Including this information in the Framework itself will be counterproductive.
- We recommend that guidelines be provided so that organizations that have had little to no experience with training can, at the very least, have a starting point. This is especially helpful for the SMB community that may not have the background knowledge and very often the resources needed, to vet various training options. We are aware that NIST will not and should not pick specific training vendors to recommend. Instead, we suggest including a listing of topics that should be covered by training for the various tier levels.
- There is currently no forum for the free exchange of ideas. While valuable, the NIST CsF Industry Resources Website has limited content, and the addition of such content is strictly controlled by NIST. Case studies or similar accounts of an organization's experience implementing the NIST CsF could help other organization's leverage lessons learned by early adopters of the Framework.
- Finally, [The organization] and its members have found resources included under "Industry Resources" on the Framework's webpage to be the most useful as we consider the form and content of Cybersecurity Framework for the Restaurant Industry.
- Nevertheless, as noted previously, NIST, and for that matter other federal agencies, could drive additional use of the Framework and best practices by providing more real world examples of the application and use of the Framework, demonstrating the business value proposition of the framework and developing incentives for its use. Just as importantly, the government can best promote cyber best practices by avoiding prescriptive regulatory regimes
- A call to action for formal case studies should be in order here with a consistent template. These can be posted for viewing on the NIST site.

Representative Questions:

- Should additional guidance about Framework use come from your sector, the government, or other organizations?
- What is the best communication mechanism for developing, sharing, educating, and discussing Framework guidance?

Challenges in Sharing Best Practices

There is a need for additional sharing of best practices surrounding use of the Framework.

Associated Key Terms/Phrases:

- Best Practices
- Lessons Learned
- Information Sharing
- Safe Harbor
- Information Repository / Forum

RFI Response Examples:

- There is no method or means to communicate how or why the Framework "work" in real life to better the cybersecurity posture of a particular company.
- Sharing of best practice requires time commitment and not every organization or every individual is able to afford to break away from their daily work. Limited human bandwidth and availability of expertise is one of the main reasons why best practices are not shared.
- …in a competitive market there is often little incentive for firms to share their best practices with other firms and how they learned from past failures to implement best practices.
- The lack of safe harbor provisions for best practice implementation and good faith efforts has also lead to a mentality among healthcare providers that has paralyzed them with fear and given the variety of interpretations to the NIST framework by regulatory agencies; the risk of not moving forward is less than the risk of potential misstep.
- A single repository to search for available best practices reports for each of the respective sectors would help address this gap.
- More emphasis on producing use cases and lessons learned documents should be made clear as the Framework moves forward.
- Liability, whether legal or otherwise, is most inhibiting the sharing of best practices.
- [The organization] believes that one of the best steps the U.S. Government can take to increase the sharing of best practices is to promote alignment of federal information security practices with the Framework Core. A majority of information security vendors service both the public and private sectors. Aligning Federal Information Security Management Act requirements with the Framework subcategories, and mapping these requirements to other global standards referenced in the Framework, will enable more vendors to compete in the public and private sector information security marketplace, driving further innovation and improving security capabilities.
- The future success of the Framework will depend in large part on the extent to which individual enterprises share their experiences and learn from the experience of others. NIST can play an important role in developing a structured program and repository to capture information on a wide array of Framework implementation considerations, including among other things, guidance on approaches to cost-benefit analyses, internal and external stakeholder communications, updated technical informative references and their applicability to the Framework, use of the core, profile and tier constructs, regulatory alignment, and innovative uses of the Framework.
- Not all critical infrastructure organizations have qualified workforce and resources to develop and implement a comprehensive security strategy, let alone possess the capacity to share best practices in cyber risk management. This is particularly challenging for small and medium-sized organizations who lack resources to keep up with latest advances in cybersecurity.

Representative Questions:

- What constitutes a best practice?
- Are automated indicators a mechanism that can be leveraged for sharing?
- Are there ways to express best practices that make them easier to integrate into a Framework-based operation?
- What is the best way to align Federal Information Security Management Act requirements with Framework (e.g., mapping SP 800-53 security controls, mapping FISMA language, restructuring Subcategories or Categories)?
- How can the government encourage and assist organizations in sharing Framework lessons learned?
- How often should events occur to share Framework user experiences? Which organizations should host those events?
- Does the proficiency of the workforce affect your ability to share or apply best practices?

d. General Themes

Regulation

Many users of the Framework say that regulation is a necessary consideration in the development of their cybersecurity programs and caution about the potential negative impact of additional regulatory requirements.

Associated Key Terms/Phrases:

- No regulation
- Compliance
- Overlap
- Flexible

RFI Response Examples:

- Broader adoption of the framework as a regulatory tool, not as a regulation, will have a significantly positive impact [on] the level of effort an organization deploys against the regulatory burden. As intended, the framework enables an organization to assess once and then to report to multiple regulators. As a voluntary program, an organization should not be forced to adopt the framework. However, especially in regulated industries, broad acceptance of the framework by the regulators will enable organizations to minimize their costs associated with complying with their regulatory burden. In other words, it is recommended that regulators collaborate together to accept a single instance of measurement for one industry member and the regulators use that information individually to conduct their regulatory assessment.
- Greater outreach to Federal (including independent agencies), State, and local regulators, is required to help alleviate the creation of regulations that are duplicative or conflicting with the current processes and/or with the Framework. Such outreach may have many forms including individual meetings, conferences, facilitated workshops, and other means. Collecting and making available industry case studies and sharing those with the respective regulators could also benefit this process.
- Consequently, to prevent duplication, it appears necessary to permit the Framework to remain flexible enough for implementing firms to add to, delete from, or modify components as necessary to ensure compliance with applicable regulations and standards while still following its spirit.
- Continued focus on reducing the overlap of existing laws and regulations with an eye on regulatory harmony across all agencies.
- If each regulatory agency was to initiate a project to map their regulations to the Framework, they would be able to see which are duplicative, unique or do not map at all. While some regulations or their implementation items may not map directly, there will be many that will. Those that do will allow agencies to be able to compare their results and provide a potential means for identifying duplication.
- A task force to review each of these regulations and their stated purposes with respect to the NIST CORE requirements would be helpful to reconcile conflicting regulations and requirements with prioritization of these in a manner that states clearly not only the desired outcome of the practice but the risk factors of not adhering to the practice. This would greatly reduce the number of risk assessments that are performed by the credit union, reduce confusion and result in stronger security.
- To moderate regulatory momentum away from the NIST Cybersecurity Framework, NIST should convene each industry and each industry's common regulatory agencies to collaboratively pursue regulatory harmonization with the NIST Cybersecurity Framework. While fulfilling a needed leadership role as convener and facilitator, NIST could then also act as an advisor to encourage appropriate harmonization or analogous tools to correspond with the NIST Cybersecurity Framework. This effort would also fulfill the directive from the "Cybersecurity Enhancement Act of 2014" to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes."

Representative Questions:

- How should the government work with regulators to ensure a harmonized cybersecurity landscape?
- What confidence mechanisms can be used to demonstrate Framework fulfillment?
- What are methods to ease regulatory burden using the Framework?

International Alignment

The Framework is gaining traction internationally but still needs continued outreach.

Associated Key Terms/Phrases:

- Continued Outreach
- State Department
- Cooperation
- International Standard

RFI Response Examples:

- Add a section in the NIST CsF document that compares, contrasts and ultimately integrates the ISO/IEC 27001:2013 information security management system requirements into the Framework.
- In addition, to further promote global awareness and adoption of the Framework, NIST should consider submitting the Framework as an international standard. Recognition by a standards organization would bolster the Framework's credibility among international constituencies and help to ensure that other countries considering cybersecurity regulations opt for a standards based approach.
- Multinational organization using the BS7799 model. NIST could continue to maintain a US version of the framework for US consensus input to the international oversight. This is important since the framework is used by US government agencies. The United Nations cybersecurity division could be a forum for international cooperation and coordination.
- As new standards and sector specific guidelines and practices are developed in the US and internationally, they need to be referenced in the CSF. For the communications sector this includes the International Telecommunications Union (ITU) and other standards and industry forums (e.g., Alliance for Telecommunications Industry Solutions (ATIS)).
- To facilitate further global adoption, NIST and its Federal agency partners should promote the Framework approach with their global government partners.
- Likewise, the White House should highlight the Framework in its strategic cybersecurity partnerships. As a globally respected government and industry partner, NIST should also continue to facilitate a range of conversations to support implementation of the Framework in the United States and beyond.
- NIST can take an important step towards increasing international alignment and integration by holding at least one, and preferably more than one, feedback meeting co-hosted by NIST, or another US government agency, along with foreign partners in an international location.
- Our view is, in such context, that the NIST Framework should be much more aggressively promoted internationally. In promoting it internationally, [The organization] recommends NIST considers enhancing the Framework from its original intention, i.e. critical infrastructure protection.

Representative Questions:

- Through what venues should the government continue international outreach (e.g., standards bodies, government dialog, industry outreach)?
- What level of alignment offers the most value (Policy, regulation, subcategories, etc.)?

Awareness

Much progress has been made in spreading Framework awareness, but more is still needed.

Associated Key Terms/Phrases:

- Progress
- Gaining Traction

RFI Response Examples:

- [The organization] urges NIST to explore ways to leverage the proposed budget increase, and the widespread recognition of the need for cyber awareness, to promote the widespread use of the Cybersecurity Framework. NIST has done excellent work promoting the Framework to date, as reflected in the increasing awareness of the Framework. However, more progress can be made. Accordingly, [The organization] urges NIST to utilize this process to review the Framework as well as opportunities from the proposed budget increase to raise awareness and promote the use of the Framework.
- Awareness of the Framework is extensive within the health insurance industry. The Framework serves as a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks. In our direct experience, its blueprint is being used to improve cybersecurity risk management, as intended.
- Based upon input from its members, [The organization] infers that there is modest awareness of the Framework in the healthcare sector.
- [U]se of the Framework could be increased with additional outreach by NIST – including through attendance at sector-specific industry conferences and facilitation of more information sharing on specific best practices and peer benchmarks.
- There is not enough awareness from the transportation sector. For many transportation agencies, the development and implementation of the Framework is not yet on their priority list of things to do and is competing with the day-to-day operations (i.e. capital and safety projects, traffic operations programs, emergency maintenance operations etc.) activities of the State Department of Transportation agencies.
- These communications and the entire process for creating the Framework, starting with the President's Executive Order, has raised awareness among senior management in the oil and natural gas industry and highlighted the importance of cybersecurity in protecting critical infrastructure.
- Education and awareness remain major barriers to improved cybersecurity for small businesses
- Since the framework's release, industry has demonstrated its commitment to using it. Many associations are creating resources for their members and holding events across the country and taking other initiatives to promote cybersecurity education and awareness of the framework
- Use of the Framework has been limited, at least in part, by a general lack of awareness of cybersecurity issues in the public safety community.

Representative Questions:

- Where should the government focus its outreach and awareness efforts?
- What can the government do to reach the broadest and most critical audiences?
- What role should industry play in raising awareness?