Response to the NIST Request for Information

Views on the Framework for Improving Critical Infrastructure Cybersecurity

Carnegie Mellon University
Software Engineering Institute
CERT Division

February 2016

1. Describe your organization and its interest in the Framework.

   Our response to questions 1 and 2 are combined below.

2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

   The Software Engineering Institute (SEI) is a Federally Funded Research and Development Center administratively homed at Carnegie Mellon University. The CERT® Division is the part of the SEI that focuses on identifying and solving the nation's cybersecurity challenges.

   CERT Division of the Software Engineering Institute

   The CERT Division has over a decade of practical experience in the successful development of models and frameworks that help organizations measure, implement, and improve cybersecurity practices. Our goal is to enable organizations to transform uncertainties into manageable operational risks and then to efficiently manage those risks. We achieve this by using data and scientific rigor in our analysis of data to drive the development and use of our products and services. As a well-established trusted resource, we also strive to improve the state of the nation's critical infrastructure owners' and operators' resilience practices.

   The knowledge and experience within the broader SEI provides us with immediate access to subject-matter experts in software engineering process improvement, malware detection and analysis, digital forensics, secure coding practices, insider threat, and cyber workforce development. In addition, we are located and work with world-renowned faculty and students on Carnegie Mellon University's main campus.

   One of the SEI's objectives is to help organizations better understand and manage cybersecurity risk and resilience. In our work with industry partners and the critical infrastructure and key resources (CIKR) owners and operators, we see the NIST work on the Cybersecurity Framework (Framework) as an essential activity in support of building improved resilience and cyber-risk management capabilities domestically and internationally.

3. If your organization uses the Framework, how do you use it (e.g., internal management and communications, vendor management, C-suite communication)?

   The Framework supports our efforts to improve U.S. resilience and establishes a common source for an industry-agnostic approach to managing cybersecurity. By having this common point of reference, we can be more effective in establishing and communicating risk-management methodologies that organizations can use to strengthen their cybersecurity practices. For example, we developed a number of assessment techniques that are used to manage cybersecurity, supply chain, and operational resilience capabilities. The Framework allows us to provide assessment results that can be mapped to or reported in the context of the Framework and the common perspective it represents.

® CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

4. What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?

   The Framework has provided valuable leadership in advancing efforts to make cybersecurity risk management and resilience practices more accessible to a wide array of organizations. We have found the Framework broadly useful and encourage continued efforts to refine and improve it.

5. What portions of the Framework are most useful?

   The structured approach jointly developed by public and private organizations has delivered strong value on the initial promise of the EO 13636 and PPD 21.

6. What portions of the Framework are least useful?

   1. The organization of the Framework mixes strategic high-level practices with more detailed activities, in particular, at the sub-category level. The varied level of practices may conflate the relative importance of the cybersecurity practices provided.
   2. The Framework does not adequately provide practices for managing supply chain (aka external dependency, third-party) risks, one of the most challenging exposures organizations face today.
   3. The Tier concepts require further clarification and guidance on their use and their relationship to other similar organizing concepts currently in use by organizations, such as maturity.
   4. The Framework does not adequately provide information or linkages to similar/related international efforts to manage cybersecurity. While international standards, guidelines, and practices are referenced in the Framework, those citations do not provide the level of organization needed to meet the global challenge.

7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?

   NA

8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.

   NA

9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?

   The challenges with regulations are a broader issue that may be best addressed separately. A key value of the Framework is its voluntary focus and use of a risk-based approach. Because

there can be a number of unintended consequences and challenges associated with a reliance on regulation to address cybersecurity risk and resilience, the Framework's voluntary and flexible approach provides a valuable non-mandated resource.

10. Should the Framework be updated? Why or why not?

    Yes. An update to the Framework would be useful and required in the context of the dynamic nature of the challenge. As change occurs and improvements are identified, the Framework must continue to evolve to remain relevant.

    It may be useful to establish a process for managing changes and providing users a more defined understanding of what areas of the Framework are likely to evolve and which areas are not going to change significantly.

11. What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

    1. With expanded use and adoption, the Framework content will require updates and refinement based on feedback from users.
    2. Provide additional guidance or use cases that offer assistance with how the Framework should be used.
    3. Expand and refine the guidance on the use and benefits of the Implementation Tiers.
    4. Due to the importance of Governance (ID.GV) to the overall success of managing cybersecurity and implementing the Framework, it would be useful to provide more information and guidance in that area.
    5. 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.

12. Are there additions, updates, or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

    It may be more productive to focus on refining the framework to be more broadly adopted and useful to organizations versus attempting to maintain references to outside resources. While that effort has value, it may be better addressed by outside users and organizations.

13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework?

    It may be useful to collect and make available industry-agnostic use-cases that include examples of lessons learned, tradeoffs, benefits achieved etcetera, as organizations implement and use the Framework. More sector-specific information may be best left to sector organizations to identify and document.

14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?

    The roadmap areas identified initially appear to be high-potential improvements. They should be revisited and prioritized with the option to add/refine them.

15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

    Because the approach of the Framework is to provide a *guide* to managing cybersecurity risks rather than a mandate, a Framework update process would be minimally disruptive. Moreover, because many anticipate that the Framework will evolve with use and feedback, a systematic update process is a logical next step to broader adoption and support.

    The best approach to an update may be to stress that the processes and methodologies in the Framework can be used in a modular manner. For example, supply chain or international content could be added in the form of new categories or subcategories to minimize changes to the version of the Framework released in 2014.

16. Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

    The information shared by NIST has helped build support for the viability and direction of the Framework. In general, the outcome for the Framework as a result of the information sharing/communication by NIST has led to broad awareness and dialogue. It would be useful to expand on this communication and information sharing both domestically and internationally to build broader support and engagement.

17. What, if anything, is inhibiting the sharing of best practices?

    A key limitation to establishing "best" practices is the diversity of variables that make one practice best for some and less so for others. The concept of best practices may be better described as leading practices.

18. What steps could the U.S. government take to increase sharing of best practices?

    The answer to this question is out of scope for this response. While the Framework can assist in this area, it may be more productive to focus on improvements to its content.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

    Considerable effort is being expended in the information sharing arena on a number of fronts (technical, threats, practices). It may be useful to review those activities to identify areas/activities that are most useful to help determine how to proceed most effectively with

information sharing that is directly applicable to the Framework (e.g., lessons learned from Framework adoption, leading practices etc.).

20. What should be the private sector's involvement in the future governance of the Framework?

    Continued partnership between stakeholders in the private and public sectors is essential. Additionally, a concerted effort to gather input from international stakeholders on the content of the Framework and the governance process is foundational to establishing the necessary engagement to support the longer term evolution of an effective set of global, cybersecurity risk-management programs and practices.

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

    Yes, such a move is a worthy consideration that merits study by a representative group of stakeholders.

22. If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

    See 21.

23. If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

    See 21.

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

    See 21.

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

    This question includes some valuable considerations that should be utilized when determining the future direction of the Framework, in particular, global alignments. Further study by key stakeholders should be conducted and recommendations made.

    It should be noted that many standards-setting organizations have chosen to integrate with global standards such as ISO, which suggests that global coordination is a key consideration. Large global organizations are keenly interested in supporting international standards to simplify their world-wide management challenges and commitments.