February 9, 2016

RSA, The Security Division of EMC, response to “Views on the Framework for Improving Critical Infrastructure Cybersecurity”

RSA Contact: Tim Shea | tshea@rsa.com | 781-515-5112

Online submissions in electronic form may be sent to cyberframework@nist.gov in any of the following formats: HTML; ASCII; Word; RTF; or PDF. Please include your name and your organization's name (if any), and cite “Views on the Framework for Improving Critical Infrastructure Cybersecurity” in all correspondence.

Use of the Framework

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

ITsec firm embracing the framework as an internal risk management tool (deploy 1H 2016) and to align our product/service offerings and go-to-market (GTM) efforts to the framework.

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.

This consolidated response effort included security practitioners, who use the framework, subject matter experts and resources from our GTM teams. We have tried to indicate the perspective of our responses below.

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

Internally our intention is to utilize the framework for internal management and communications, vendor management, and executive communication.

Our customers who are adopting the framework generally intend to use the framework in two ways. The first is in the intended sense describe by the framework document (know what is in a cybersecurity program, assess yourself against it, remediate, track progress). The second use they are interested in is a measurement to share amongst partners – a way to communicate their cybersecurity posture or to have prospective partners convey their cybersecurity posture to them.

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

5. What portions of the Framework are most useful?

From our customer framework engagements: The GAP analysis and resulting roadmap. By assigning budget to the GAPS (cost to close) we developed an effective ROI tool to help prioritize the roadmap. Our customers also state it allows for direct communications and common taxonomy between practitioners, C-Suite and Boardroom.

6. What portions of the Framework are least useful?

Privacy methodology, which is currently underdeveloped. In our customer engagements it has also been the least leveraged portion of the framework.

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)?

Our internal use of the framework has been delayed by internal factors.

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.

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? [7]

The E.O. instructs the regulators to leverage the framework as part of their regulatory efforts. Broader adoption of the framework as a regulatory tool, not as a regulation, will have a significantly positive impact 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. Additionally, it is recommended this practice be international in scope.

Possible Framework Updates

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

We believe that the stability of the framework is an important factor in enabling adoption of the framework. Significant changes to the framework will create a moving target for adopters, increasing the cost and complexity of adoption. Based on customer interaction, we believe this to be particularly true for smaller organizations. We don't think that significant changes to the framework should be contemplated in the near term or until the framework has been successfully transitioned to the private sector.

There are four topics which would be appropriate to include at the next workshop. These topics reflect enhancements to or capabilities which will benefit the framework. The four topics are: additional industry-specific mappings in the informative references; additional clarity to the framework tiers; the importance of leveraging the framework down the supply chain and; need for a reference architecture to support the framework.

1. NERC, HIPAA & PCI DSS are examples of three industry-specific informative references which offer a broad mapping to the framework and would impact a large number of potential adopters. In particular, for small to medium sized organizations, additional informative references, which map broadly to the framework, would help reduce the cost and time of adoption.

2. In working with customers, the framework component generates the most discussion is the tiers. There are two reasons for this. First, a given tier is a subjective ranking based on one's perception of risks against a specific asset. Second, similar GAP analysis ranks for two subcategories imply a similar level of effort to close those GAPs. The fact is that a GAP of -1 in one subcategory might require a significantly different level of effort and resource than a GAP of -1 for a different subcategory. Development of a tool(s) which would help to provide additional visibility into the work required, and progress against, closing GAPs would be of benefit.

3. A cybersecurity program is only as strong as its weakest link. The value of extending the framework to one's supply chain cannot be underestimated. The benefits include better cybersecurity and the ability to demonstrate Due Care in the case of a breach and litigation.

4. The framework delivers a set of best practices and standards with which an organization can describe and measure its cyber risk management program. What the framework lacks is a fabric which nits the framework to operational capabilities.
    - Thus, to help drive adoption of the framework, we would like to see the development of a detailed reference architecture (the fabric), which provides a roadmap to

operationalize the framework. This reference architecture should provide three operational views. These views would include technology, systems and operations (process).

    - Technology would be the categories of ITsec HW and SW tools which would be deployed.
    - Systems are how the tools are configured and deployed into capabilities.
    - Operations (process) is the workflow associated with operating the resulting cyber capabilities.

- This reference architecture also serves to highlight the interdependencies in capability required to leverage the functions, tiers, profiles and informative references in the framework.
- This reference architecture, in conjunction with the institutionalization of the framework, enables an organization to achieve a higher state of awareness and capability. The objective is to enable an organization not just to Recover from a cyber incident but to be Resilient when faced with a cyber incident. Recover suggests that systems are down, you revert to a previous known best state, fix the problem and bring the systems back up. Resilience suggests that in the face of a cyber event, one has architectural options which can be deployed to both negate the cyber event and maintain operational capability of the attacked systems.
    - The institutionalization of the framework ensures an adaptable and repeatable process with which to assess capability and risk which will then, in turn, inform decisions on how best to leverage the reference architecture.
        - We should continue to look towards drivers for the adoption and institutionalization of the framework, to include incentives and regulatory activity.
- This reference architecture addresses activities which U.S. Government can take to increase sharing of best practices (question #18 below).

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.

- Additional clarity on tiers and level of effort associated with closing GAPs
- Additional industry-specific informative references (especially those that have broad mapping to the framework and are appropriate for critical infrastructure)

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?

Two related comments:

A methodology for capturing and then measuring progress with regards to the level of effort required to close a GAP would helpful. Point being that the level of effort and number of steps required to close a GAP of ‘1’ for subcategory A might be significantly different that a GAP of ‘1’ for subcategory B.

For the organizations that want to use the framework to share their posture or “measure” the posture of partners, it is a recurring theme that they are looking for some sort of quantitative, objective “scorecard” kind of template for sharing and comparing their results.

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?

14. Should developments made in the nine areas identified by NIST in its Framework-related “Roadmap” [8] be used to inform any updates to the Framework? If so, how?

Yes, specifically the addition of supply chain appropriate informative references in support of 4.8 - Supply Chain Risk Management.

In our customer facing framework engagements we find that roughly 50% of the customers are headquartered internationally or are an international organization. They understand that the framework is a U.S. driven initiative. Nonetheless, they are looking to rationalize the framework with other international initiatives, such as the U.K. Cyber Essentials scheme. Section 4.7 of the NIST Roadmap for Improving Critical Infrastructure Cybersecurity calls for the alignment of the framework with other international efforts. Based on our experience with customers we believe this is a roadmap item which could use additional focus.

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

Minimize changes to the three components (Core, Tiers, Profile)

Sharing Information on Using the Framework

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?

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

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

The Government should collaborate with the sixteen critical infrastructure segments to development a detailed reference architecture which describes how to operationalize the framework.

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)?

Private Sector Involvement in the Future Governance of the Framework

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

Ultimately the private sector should own the framework and be the governance vehicle.

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

Yes, all.

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

The framework should be transitioned in total. Breaking it apart, with multiple governance vehicles, would likely dilute or make the framework less coherent and functional.

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?

For profit or not for profit is less important than the framework remaining free to users. As a U.S. driven initiative, an organization based in the U.S. but with international reach would be preferable. It's also important that NIST have a role in this organization. Not on the governance side but rather as an intermediary back to the U.S. Government and its objectives for cyber risk management as well as to maintain NISTs role in promoting and supporting the framework.

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?

In question #10 we recommended against updates to the framework. To be more specific, once the framework has made a successful transition to a private entity, updates could be considered. We would argue that there are no changes to the framework itself for at least 12 months prior to transition, as likely 12 months post transition. This will enable those implementing the framework to minimize the invariable disruption associated with such a transition.

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?

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