David J. Leigh
7960 Donegan Drive
Suite 225
Manassas, VA 20109
dleigh@RoforiCorp.com

February 9, 2016

Subject: Rofori Corporation "Views on the Framework for Improving Critical Infrastructure Cybersecurity"

Rofori Corporation is pleased to submit its response to NIST RFI 80 FR 76934, "Views on the Framework for Improving Critical Infrastructure Cybersecurity". Rofori Corporation offers an approach and software solution to **measure** an organization's cybersecurity risk posture, including its supply chain, utilizing the Framework Core and Target Profile as the central foundation. DEFCON CYBER™ employs the Framework Target Profile, at the Subcategory level, as a representation of an organization's ***strategy*** (i.e., actions to achieve an aim) for protecting its critical assets from its high impact threats. From a prioritized Target Profile, an organization is positioned for measurement as to the strength of its cybersecurity strategy and its ability to execute its strategy with respect to responsiveness and effectiveness. Along with these two critical components, risk representations for the critical assets, threats, and other execution characteristics are used to compute a continuous holistic cybersecurity risk posture score.

DEFCON CYBER™ is available today as a Cloud service or an on premise Microsoft SharePoint application add-in (www.DEFCONCYBER.com).

RFI RESPONSE:

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

   Rofori Corporation has two (2) perspectives of the NIST Cybersecurity Framework (Framework):

   - As a small cloud services and software solutions company, we desire to manage our cybersecurity risks through continuous measurement and improvement as part of our Enterprise Risk Management process using the Framework.
   - As a solutions product company we see the Framework as the foundation for our cybersecurity risk posture measurement product, DEFCON CYBER™, with the Framework **enabling**:
     - A Common language (i.e., Rosetta Stone)
     - A Consensus definition of "best practices"
     - A Risk management approach to cybersecurity
     - Bridging the gap between the Technical and Business domains leading to informed business risk decisions
     - Prioritization of all aspects of the cybersecurity program, including indicators of Compromise, Vulnerability, Threats (threat intelligence), and other critical actions (such as, change/access/inventory management, categorization, network design & segmentation, etc.)
     - The Representation of an organization's cybersecurity risk mitigation strategy (i.e., Target Profile prioritized at the Subcategory level)
     - Cybersecurity outcome and Risk Posture **measurement**

Given that Framework Subcategories represent "Best Practice Outcomes", and given that a best practice outcome in cybersecurity cannot be achieved without taking action, it follows that a best practice outcome can only be achieved as a result of an activity or process performed by the organization. The Framework Target Profile thus represents the outcomes that an organization needs to achieve through its actions in order to protect its critical assets from the highly likely and impactful threats at a given level of risk. This represents a significant portion of a risk mitigation strategy – actions to achieve an aim.

DEFCON CYBER™ goes well beyond periodic cybersecurity program "Assessment", "Auditing", and "Scoring". DEFCON CYBER™ provides a **continuous** holistic score that **measures** the critical elements of the organization's Cybersecurity Risk Posture from Asset, Threats, and Operations components: such as the strength of its cybersecurity risk mitigation strategy, the ability of the organization to execute their strategy, time to respond, and the cumulative risk posture of its supply chain.

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.

   I am responding as a Framework user and as a Subject Matter Expert.

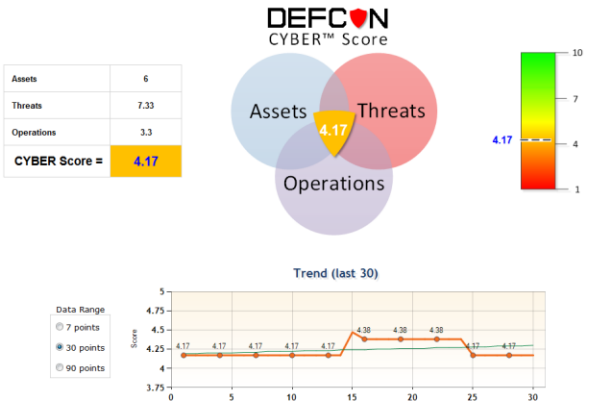
   I am also representing several organizations that are adopting the Framework and applying it to their cybersecurity programs, desiring to improve their cybersecurity outcomes through continuous risk posture measurement.

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

   1. As a cloud services and software product company, we use the Framework as the overarching cybersecurity risk management approach for measuring and managing our cybersecurity risks. Using the Framework in February 2014 for a Board and executive briefing was the first time our non-technical members fully understood why cybersecurity was important and what good cybersecurity meant. During this discussion, we realized that cybersecurity measurement could, and should, be made at the Risk Posture level, and the Framework provides the "framework" for doing so. We applied the Framework approach to our own organization and it has become a focus for cybersecurity improvement across the entire organization – you can't manage what you don't measure.

   2. An additional result of our February 2014 Board and executive briefing was a decision to produce a software solution to position any organization for holistic, continuous, transparent, and standards based cybersecurity risk posture measurement, the DEFCON CYBER™ Score.

      *We use the Framework as the core of DEFCON CYBER™ from which to represent a **prioritized risk mitigation strategy**: actions to achieve an aim, which is, the actions you need to perform well in order to protect your critical assets from your threats.*



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

   The most effective portions of the Framework are the Core and Profiles. They form the basis of a risk mitigation strategy, and the foundation for prioritization, operationalization, and measurement.

   Generally, we have encountered 4 kinds of organizations:

   1. Actively using the Framework to align and gather information in a survey / assessment (spreadsheet) style of approach. Typically it is the compliance or risk management group that is attempting to align the cybersecurity program throughout the organization and identify gaps, or heuristic risk assessment.
   2. Aware of the Framework, but not actively using it. Many of these small to medium sized organizations, law firms, insurance/risk firms, and other consulting organizations, typically don't know how to get started or what to do next.
   3. Have heard of the Framework, but are confused as to its purpose or relationship to other standards and technical controls.
   4. Never heard of the Framework.

   All organizations we have encountered have not been able to transition from a compliance attitude to an operationalized risk management approach using the Framework to solve the paramount issues facing every organization, how to prioritize their efforts, how to decrease the noise from their security tools and information feeds, and how to **measure** cybersecurity effectiveness.

   In our discussions, many organizations do see the value DEFCON CYBER™ brings to their organization for operationalizing cybersecurity risk management through cybersecurity posture measurement.

5. What portions of the Framework are most useful?

   Core and Profiles at the Subcategory ("Best Practice Outcomes") level.

6. What portions of the Framework are least useful?

   Implementation Tiers seems incomplete or immature. With the definition of Implementation Tier being,

   > "A lens through which to view the characteristics of an organization's approach to risk — how an organization views cybersecurity risk and the processes in place to **manage** that risk."

   DEFCON CYBER™ is able to **measure** the organizations aptitude for cybersecurity risk **management**, including its risk mitigation actions, without using the concept of Implementation Tiers at this time.

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)?

   Lack of awareness in industry about the Framework, and the absence of metrics, data supporting best practice, and lack of guidance for how to use the Framework for "improving the security and resilience of critical infrastructure."

What does "improving the security and resilience of critical infrastructure" mean if it is not objectively defined? Without effective measurement, you don't have an indication of where you are or if you are approaching your objective, or not. Without effective measurement of cybersecurity and outcomes, along with supporting data, there can be no meaningful, or objective, evaluation of improvement in the "security and resilience of critical infrastructure".

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.

   The Framework has enabled our firm to implement an effective cybersecurity risk management program incorporated into our Enterprise Risk Management process resulting in business risk mitigation actions leading to a 60% improvement in our DEFCON CYBER™ cybersecurity risk posture Score.

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?

   Continue to support and expand the mapping of other "regulatory requirements, mandatory standards, and related processes" into the Framework Core. Assess and incorporate industry innovations into the Framework.

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

    Yes 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 (see item 11), they are not of sufficient magnitude or value to warrant the effort expended to produce an update at this time.

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.

    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.

    We would suggest that NIST focus on **practical** implementation of the Framework, not necessarily the unproven "next big thing" (e.g., big data analytics), because good execution of a strategy, even a weak one, generally produces better outcomes than poor execution of a brilliant strategy. It is our small and medium sized organizations that need guidance and recommendations for improving their cybersecurity risk postures. In the NIST Supply Chain cybersecurity workshops, many organizations with significant numbers of supply chain entities agreed that cybersecurity risk posture would be significantly improved "if only we knew our supply chain was performing basic system hygiene well."

    We believe that the broad deployment of the DEFCON CYBER™ approach will result in the objective measurement of cybersecurity risk posture for an organization and its supply chain, incorporating the scope and effectiveness of its strategy and execution.

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?

    Incorporate updated references to Common Security Controls Version 6.

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?

    Yes. Examples and **recommended** target profiles for different industries and organization sizes should be incorporated into the Framework as an implementation guide. One example of particular value is the FCC CSRIC working group 4 recommended target profiles and challenges to implementation sections for "small business" communications firms.

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?

    Yes, some of the nine areas are more important now than others. Specifically, 4.3. Conformity Assessment and 4.8. Supply Chain Risk Management are of particular importance with respect to cybersecurity risk **measurement**. DEFCON CYBER™ is an industry solution for these areas.

    We would like NIST to focus on resources pertaining to awareness of the Framework, and practical/effective implementation of the Framework at this time.

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

    Approach updates as "enhancements" and not a restructuring.

16. Has information that has been shared by NIST or others affected your use of 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?

    All has been informative.

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

    Documentation of use cases, data, measurement, and metrics.

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

    Utilize existing resources, such as the National Cybersecurity of Excellence (NCCoE), to pilot, evaluate, and assess innovation and new approaches for **measurement**, metrics, and data supporting "best practices".

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)?

    Liability protection, actual value to the sharing organization.

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

    The same as with its creation, collaboration. The open Workshop and review process enabled any organization, large or small, to participate. The resulting Framework is as valuable as it is because of the process NIST employed to create it. This process should be continued.

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

    An emphatic NO! NIST is a trusted entity for organizations in the U.S., and all of the work products are freely available. This must continue to be available to small and medium sized U.S. firms.

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?

    Retain the open Workshop and public review process, and make the Framework and all supporting materials publically available at no cost.

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?

    N/A

Sincerely,

David J. Leigh
President & Co-Founder
Rofori Corporation / DEFCON CYBER™