CREATe.org
Center for Responsible Enterprise And Trade

To: Andrea Arbelaez, National Institute of Standards and Technology
From: Craig Moss and Pamela Passman, CREATe.org
Re: Comments on NIST Cybersecurity Framework V1.1
Date: 1/17/18

We appreciate the opportunity to comment on the revision. As background, CREATe formed a Cybersecurity Advisory Council in 2016 consisting of 25+ large companies and universities. The mission of the Advisory Council is to accelerate the adoption of the NIST Framework, with a focus on its application in global supply chains.

Over the course of numerous group and individual meetings, four interlinked areas emerged as critical for broader adoption of the Framework:

- Scope – how do you define the scope of an assessment in a consistent and transparent manner
- Calibration – how do you calibrate assessment results so you can compare the current state of cyber risk management among organizations and/or benchmark one assessment result against others
- Verification - how do you verify self-assessment results in a cost-effective and scalable way
- Improvement – how can you establish a more direct link between the assessment results and a priority improvement road map

Given this background, here is a summary of CREATe's comments on V1.1. These comments do not reflect the stated opinions of the individual council members, but we believe they do accurately capture the collective challenges discussed by the Advisory Council. The CREATe Cybersecurity Advisory Council is continuing its mission of accelerating the adoption of the Framework in 2018. We would be happy to provide additional detail if useful. We appreciate the continued work to evolve the Framework and the significant contribution NIST has made to cybersecurity.

Comments

Overall, the increased focus on supply chain is an important positive step since cybersecurity risk extends beyond the organization to the third parties (suppliers and buyers) in an organization's ecosystem.

The overall description of supply chain risk management in section 3.3 is sound but it could provide more emphasis on the multi-level reality of supply chains and the need to look beyond direct suppliers. The goal is to help organizations to cascade cyber risk management from suppliers to sub-suppliers, etc.

Effective supply chain risk management always requires two distinct system elements, and more clarity could be added on this distinction and the relationship between the two elements:

1. What program does an organization have in place to manage cyber risk in their supply chain?
2. What program does the third party (buyer or supplier) have in place to manage cyber risk in their organization?

The addition of Supply Chain Risk Management as a category underneath Identify is a good start. However, it does not fully address the complexity of the supply chain, the risk it poses nor the essential nature of interconnectivity in today's global and digital business world.

Some of the specific Supply Chain sub-categories include too many separate tasks for an organization to assess its current state in a meaningful way, nor link the assessment response to a specific improvement plan. One example of this is: *"ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed and agreed to by organizational stakeholders."* Clearly, "identified, established, assessed, managed and agreed to" are separate activities that do not happen simultaneously.

While we appreciate the various public views about the role of the Tiers, the Tiers continue to be an area that need clearer guidance on the limits of their use. V1.1 makes the calibrated use of the Tiers more difficult by adding supply chain considerations to "External Participation" in all four Tiers. It also makes it more difficult for an organization to fully understand its current state in managing cyber risk in its supply chain or the ability of third parties in that supply chain to manage its own cyber risk.

Although the Framework continues to say that the Tiers do not "necessarily" represent maturity levels, it seems that there is more emphasis on the use of the Tiers as a measurement related to Profiles and Self-Assessments.

Each Tier has too many variables to be an effective measurement for an assessment. The number of variables in each Tier also make calibration extremely difficult. This has an additional unintended consequence of making verification much more time consuming, subjective and labor intensive than necessary.

Encouraging organizations to customize the Tiers is good in the context of each organization setting its risk tolerance, as well as understanding its related economic risk and the cost/benefit of improved cybersecurity risk management. But encouraging customization of the Tiers makes them less and less useful as a shared, calibrated measuring tool.

However, it is very encouraging to see the following inclusion in the text of the revision: *"organizations should consider leveraging existing guidance…., existing maturity models, or other sources to assist in determining their desired tier."* This could be an effective direction for

NIST to pursue further. The Tiers could act as a common foundation for maturity models that are aligned with the Framework. In pursuing this direction, NIST's Tiers could be used to gauge the equivalency between the maturity models that are developed. This would enable one organization to compare their maturity, based on their selected maturity model, with another organization's maturity, which may be based on another maturity model.

The general encouragement for organizations to customize the Framework and the Tiers is understandable and has some positive elements. It should be noted however, that it may undermine the ability for the Framework to be effective in being a resource deployed through supply chains. It may also lead to suppliers spending more time on assessments and less time on improvement. In the supply chain, one organization could be a supplier to 30 organizations. Cybersecurity in the supply chain is bi-directional, which is an important distinction from some other supply chain issues that tend to be driven from buyer to supplier in a top-down approach. If each organization customizes the Framework it creates a nightmare for the supplier. This would repeat the mistakes made in environmental and labor supply chain risk management and compliance 20 years ago. Customization of the Framework and Tiers also makes benchmarking impossible and complicates best practice sharing to some extent. Broad supply chain adoption will require improved calibration among assessment results.

The use of the Current and Target Profile continues to be a strong area, however, their needs to be a stronger linkage between the Profiles and a calibrated measurement – especially for use in the supply chain. The use of Profiles would be enhanced by more guidance on determining the scope of the assessment, which is so critical to benchmarking and even tracking improvement over time.

The inclusion of the Self-Assessment is a positive step, as is the increased attention to linking the risk assessment to driving improvement and cost/benefit analysis. However, concerning improvement, there is a lack of clarity about how to determine if the outcome is being "partially" or "fully" achieved.