https://NavigationAdvisors.com

January 19, 2018

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Comments on Draft 2 of the proposed update to the NIST Framework for Improving Critical Infrastructure Cybersecurity (version 1.1)

Thank you for the invitation to provide comments on Draft 2 of the Cybersecurity Framework for Improving Critical Infrastructure (the "Framework") version 1.1 and the proposed update to the Roadmap for Improving Critical Infrastructure Cybersecurity (the "Roadmap").

We appreciate the deep expertise and the systematic collaborative approach to developing and updating the Framework that NIST has consistently demonstrated. Your changing the initial version of the draft to take into account some of the comments and suggestions submitted in 2017 is a reflection of this approach and of your commitment to working together with the industry, academia, and other stakeholders.

The Cybersecurity Framework has become the foundation of cyber risk management for numerous enterprises. It has informed many decisions in cybersecurity and the broader field of cyber risk management. The comments below are limited to selected aspects of the proposed Framework update. We intentionally focus only on potential areas of improvement; this focus should not be seen as a negative view of any element of the proposed update to the Framework. The primary points of the comments are the following:

- The NIST Cybersecurity Framework has had a significant positive impact on the cybersecurity of the critical infrastructure and of society as a whole. Updating and expanding the Framework can increase this impact.

- Reducing the scope of the section on risk measurement and quantification (now labeled "Self-Assessing Cybersecurity Risk with the Framework") compared to the previous draft is the right practical solution to avoid delays in moving forward with the new version of the Framework.

- This reduction in the scope of the section on risk measurement and quantification is, however, no more than a temporary measure until additional work on risk measurement and quantification can be done. Without such content, the Framework will still be missing a critical component that should contextualize and anchor most of its other elements. There is a clear need for further emphasis on cyber risk measurement and cyber risk quantification.

- There are a number of minor changes that can further improve the readability and usability of the Framework document.
- It is important to prevent unintended consequences in the use of the Framework. Misinterpretation of the Framework's scope can lead to harmful outcomes.

Quantification of risk, risk measurement, and enabling informed decision-making

Last year we provided to you an outline of some of the problems with and potential criticism of the section "Measuring and Demonstrating Cybersecurity" (labeled "Self-Assessing Cybersecurity Risk with the Framework" in the current draft). We support your decision to revise the section and to tighten its content. Even though this change includes the elimination of most of the discussion of measures, metrics, and correlation to business results, we view it as a necessary practical solution to avoid delays in producing the next version of the Framework.

However, we see this as only a temporary solution, and hope that the Framework will in the future be expanded to include additional discussion of this important topic. The latest draft of the Roadmap indicates that this is in fact the plan NIST intends to follow. We see this next step as critical to the improvement of the Framework and its relevance in the long term. Of all areas of potential improvement, this one is arguably the most important.[1]

Measuring risk is key to managing risk. Without proper measurement of risk, it is impossible to make informed decisions on whether and how the risk should be reduced, what cybersecurity investments should be made and what activities undertaken, and what business objectives can be successfully pursued. Proper measurement of risk is a necessary element of informed decision-making in business and in making choices to best achieve organizational objectives.

In the absence of clear ways to measure risk levels, the proposed expanded use of Tiers and Profiles is a temporary solution for many enterprises, even where these Tiers and Profiles are determined based on largely qualitative assessment. The proposed changes to the Framework correctly emphasize this approach.

Cyber risk and the impact of cyber events in the context of Enterprise Risk Management

Cyber risk is rapidly growing in its importance, and managing this risk is an essential component of Enterprise Risk Management (ERM). The Framework document makes this

[1] The format of these comments does not allow us to include the level of technical detail necessary to provide specific suggestions and delineate possible options in addressing some of these challenges. We note that traditional "cybersecurity metrics," as they are typically used, do not translate into any quantitative measures of risk level needed for proper risk analysis and management. They rarely provide more than a directional view of improvements of a certain type. They generally do not lend themselves to most types of aggregation. At best, they provide limited guidance concerning the primary characteristics of risk events, i.e., the probability distributions of their occurrence and impact. Even when this guidance can be provided, it is largely based on qualitative considerations. Improvements are needed and possible; these improvements do not necessarily have to involve the often-criticized attempts to blindly apply the Value-at-Risk (VaR) approach.

general point very clearly. We note, however, that the very beginning of the Executive Summary contains the statement, "Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers." While not necessarily incorrect, the statement creates the impression that cyber risk does not overlap with other types of risk. Unfortunately, this wrong interpretation is consistent with the way it is seen by many in the industry.

In reality, cyber risk is not only interdependent with but directly overlaps many other types of risk. For example, a data breach (cyber) may result in significant reputational damage (reputational).

Specific examples include many well-publicized data breaches such as those experienced by Equifax and Target as well as the breach at the OPM.[2] Attempts to estimate the overall cost of the events have been made, including attempts to estimate the losses due to reputational damage (direct losses, decrease in brand equity, and others). Companies have seen significant financial losses, decline in competitive advantage, and reduction in future business options. In the case of some smaller companies, the effects of data breaches and other cyber events have been devastating. In some cases, cyber incidents have driven companies into bankruptcy.

We suggest that this statement in the Executive Summary be modified to properly reflect the overlap and interdependence of cyber and other types of risk, which will also emphasize that cyber risk management is part of the overall Enterprise Risk Management.

Understandability and usability of the Framework document

The intended audience of the Framework is different from that of many NIST documents on standards and best practices. It is also broader. The ability to clearly explain key concepts to all segments of this audience affects the Framework's ultimate degree of adoption.[3]

The current draft includes some unnecessary acronyms and terms. This reduces the document's readability when it is used by people who do not deal with these issues on a day-to-day basis. Difficulty in understanding the intended meaning is a relatively common reaction to some elements of the Framework, as we have witnessed in the interactions with

---

[2] https://energycommerce.house.gov/hearings/protecting-consumer-information-can-data-breaches-be-prevented provides some of the background information on the Target data breach and also illustrates the reputational damage and some other types of negative consequences from this breach. https://energycommerce.house.gov/hearings/oversight-equifax-data-breach-answers-consumers/ has some of the background information on the Equifax data breach and illustrates the reputational and other damage. https://oversight.house.gov/hearing/opm-data-breach/ has some of the initial descriptions of the U.S. Office of Personnel Management (OPM) data breach and provides an illustration of the reputational and other damage from the event.

[3] Senior management and boards of directors of many organizations are also exposed to the Framework, even if this exposure is indirect but happens through other people at the organizations. They too are affected by any lack of clarity or unnecessary complexity. In our experience, understanding of the Framework by those who set overall enterprise risk controls and risk governance is often at a very low level.

many risk management and even technical cybersecurity professionals. This is a barrier to many industry participants. There are a number of areas where the use of acronyms or unclear (to the uninitiated) terms can be reduced.[4]

In some cases the unnecessary introduction of new terms can lead to confusion, especially if these terms are defined in ways different from industry usage, or where multiple definitions currently exist. For example, the new draft introduces the term Cybersecurity Incident with a specific definition, whereas this term is often used in the industry with a different meaning.[5]

The definitions of Tiers may be too rigid, which can also affect the usability of the Framework. For example, the document appears to assume that in all cases, sharing information with others is always, without exception, indicative of higher security than not sharing internal information. "External participation" in Tier 2 (Risk Informed) does not require sharing of information externally, while it is required for Tier 3 (Repeatable) and Tier 4 (Adaptive). We suggest that the situation is actually more complex than this would indicate.

Unintended consequences of the Cybersecurity Framework

It is important to reduce the chance of unintended consequences in the practical use of the Framework. This concerns both the scope of the Framework and the way it is implemented.

The Framework has been developed for the critical infrastructure. It can also help to facilitate wider adoption of practices that can increase risk management-based cybersecurity in enterprises of any type and in any industry. The voluntary Framework itself, however, has never been intended to apply directly to enterprises outside of critical infrastructure. While the general foundation of the Framework is applicable to almost any enterprise, the Framework itself is not. This should remain very clear to all who use, are considering the use of, or are in other ways exposed to the Cybersecurity Framework.[6]

As an example of improper use of the Framework, we can point out that some insurance companies, when considering providing cyber insurance coverage, have included questions about compliance with the NIST Framework in their questionnaires. While the questions may

---

[4] For example, the acronym OT is used only once (p. 18 of the draft) other than in the list of changes and the list of acronyms in the appendix, and the meaning of the acronym is explained only in the appendix at the back. In another example, the IoT acronym is never used on its own (except in the list of acronyms) and only appears in the text in parentheses after it is spelled out. These and other seemingly small details affect the readability of the document.

[5] The definition appears to require that such an event necessitate "response and recovery." This requirement results in a much narrower definition than used by many in the industry and may create the impression that some of the cyber events currently classified by the industry as cybersecurity incidents should be reclassified. This potential negative should be considered together with the advantages of separating events and incidents in the proposed draft. Other examples also exist.

[6] It would be unfortunate if there appear new cases of overly broad application of the Framework, such as requiring certification of "full compliance" with the Framework in contracts with all suppliers as part of Supply Chain Risk Management of cyber risk. We are troubled by the occasional use of the "full compliance" with the Framework description of cybersecurity practices by some in the industry despite the fact that the Framework is not a standard or requirement.

be appropriate for certain enterprises, asking these questions of enterprises outside of the critical infrastructure creates the impression that compliance with the Framework is expected or encouraged, which is equivalent to an incentive to adopt the Framework. Where this is done for enterprises for which the Framework has not been designed, potential results can be characterized as suboptimal at best.

We note that the Roadmap includes a section focused on enterprises that are not part of the critical infrastructure as it is traditionally defined. This initiative is important and should be pursued. The work NIST has already done on the Framework can be utilized—after it has been appropriately modified—in helping to improve cybersecurity and the management of cyber risk in our society. While important on its own, this broad improvement will also have an indirect spillover effect of increasing the level of cybersecurity of the critical infrastructure.

We strongly support your activities in the development and improvement of the NIST Framework for Improving Critical Infrastructure Cybersecurity, as well as your work in educating both government agencies and the industry on issues related to the Framework and cybersecurity in general. NIST is perfectly positioned to continue providing leadership in the area of advanced cybersecurity.

Sincerely,

Alex Krutov
President
Navigation Advisors LLC
alex.krutov@navigationadvisors.com
www.navigationadvisors.com