April 9, 2017
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
(Attention: Edwin Games)

Re: Proposed update to the NIST Framework for Improving Critical Infrastructure Cybersecurity

We are pleased to offer the following comments in response to the National Institute of Standards and Technology's (NIST) request for comments on a proposed update to the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework").

Below we comment only on selected aspects of the Framework. 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:

- Significant positive impact of the NIST Cybersecurity Framework. Importance of updating the Framework.
- Need for additional emphasis on cyber risk measurement and risk quantification. Cyber and enterprise risk quantification as an essential part of risk management. Suggestion to improve on the approach used in the proposed update.
- Need for guidance on the definition of critical infrastructure in the Framework. Potential harm from misinterpretation of the Framework's scope.
- Importance of preventing unintended consequences in the use of the Framework.

Significant Positive Impact of the NIST Cybersecurity Framework. Importance of Updating the Framework

The NIST Cybersecurity Framework for Critical Infrastructure has had a significant impact on how cybersecurity is managed and cyber risk assessed since it was first introduced in 2014. It has become the foundation of cyber risk management for many enterprises. Many others have not adopted the Framework but benefited from being exposed to it. The NIST Cybersecurity Framework has informed many decisions in cybersecurity and the broader field of cyber risk management, including in some areas outside of the Critical Infrastructure.

We strongly believe the Framework is becoming an increasingly important part of cyber risk management. This makes it particularly important to continue improving the Framework and assuring that its form is most useful for improving cybersecurity. The carefully considered introduction of Version 1.1 by NIST is the right way to proceed.

NEED FOR ADDITIONAL EMPHASIS ON CYBER RISK MEASUREMENT AND RISK QUANTIFICATION. IMPORTANCE OF PROPER GUIDANCE ON RISK MEASUREMENT AND OVERALL RISK MANAGEMENT

The proposed update to the Framework to create Version 1.1 provides additional guidance on areas specific to intelligent management of risk. This is an important and necessary step.

At the same time, there are potential areas of improvement. This statement is based on the following observations:

-The added material on risk measuring and cybersecurity is not entirely consistent, and it is difficult to understand for those who are not familiar with the topic.

-In some cases, this material seems to demand certain actions and specify objectives, while not providing sufficient guidance on how these objectives can be achieved, or on what constitutes achieving them.

Complex and confusing can be simplified

Being well familiar with the topic and having experience of closely interacting with those who are not, we see the language and the way concepts are presented as difficult to understand for many cybersecurity professionals.

For example, the list of acronyms that most do not understand has been expanded in the proposed update. They also include terms that may not have been defined and, in general, have more than one definition. Examples include CPS for Cyber-physical systems and PII for Personally identifiable information, both of which have more than one general definition but are not defined in the Framework document. Additional examples include the proliferation of unnecessary acronyms such as SCRM for Supply Chain Risk Management and OT for Operational Technology. They make the relevant parts of the Framework document difficult to understand for most cybersecurity professionals and require an unnecessary investment of time and other resources.

Potential confusion is created by redefining known terms

We question the wisdom of providing definitions of terms and using terms that are not standard or generally accepted. For example, key terms such as "metrics" and "measures" are defined[1] in ways inconsistent with how these terms are used by many in the industry, and the kind of distinction between metrics and measures, as defined in the proposed update to the Framework, is not a generally accepted one.

Cyber risk management uses the same general basic terminology and concepts as any other type of risk management. Its many unique challenges have never been a reason to switch to rarely used and unexpected definitions.

[1] The definitions follow the Cybersecuritry Metrics and Measures paper published in 2009 (Cybersecuritry Metrics and Measures, Black et al, March 2009, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51292) that provides an excellent short overview of some elements of cyber risk management. That paper defines the terms in specific ways chosen to facilitate the type of analysis provided by the authors. However, this is not necessarily how the same terms are defined elsewhere or generally understood.

The existence of other definitions[2] and interpretations is particularly problematic and makes it worse than if these terms were for the first time introduced in the Framework.

Confusing terminology can lead to questionable reasoning

In addition to the confusion resulting from using restrictive and rare definitions where other definitions also exist in risk management, the particular choices of definitions themselves can drive concepts and reasoning that are questionable.

For example, “measures” are defined in the proposed update to the Framework as “quantifiable, observable, objective data supporting metrics,” while “metrics” are described as typically being “higher level, qualitative, and an aggregate of several measures.”

If metrics are an “aggregate of several [quantifiable] measures,” it is unclear why they have to be “qualitative” in nature. An aggregate of quantifiable elements can also be quantitative (as opposed to qualitative).

Simply put, something based on several numbers can often be calculated. It can be a number too, and be calculated in a defined way. This means that it does not have to be “qualitative” (as opposed to quantitative or quantifiable). In fact, one of the goals of risk management is to have the greatest degree of risk quantification and objectivity.

Advisability of revisions to the proposed update

Even if we accept how the terms are defined in the proposed update, their subsequent description can be improved. Given how much is based on these basic terms and concepts, we see this as an area where clarifications and revisions to the proposed update are advisable.

Qualitative vs. quantitative

Qualitative considerations are important in cyber risk management. Qualitative considerations play a critical role where quantitative—as opposed to qualitative—approaches are difficult to apply or cannot reduce the degree of uncertainty to acceptable levels. It happens very often. This does not change the overall goal of quantifying cyber risk to the degree it can be accomplished, and reducing reliance on educated guesses and judgment.

Some of the great places for qualitative considerations are in deciding which quantitative approaches can be utilized and how it can be done best, and in the decision-making based on proper interpretation of data.[3]

[2] Even the Wikipedia provides definitions completely different from the ones used in the proposed update. Wikipedia states, “In the context of risk measurement, a risk metric is the concept quantified by a risk measure.” It then explains, “The method or formula to calculate a risk metric is called a risk measure.” (“Risk metric,” Wikipedia, https://en.wikipedia.org/wiki/Risk_metric, Accessed Apr. 8, 2017) These definitions have nothing in common with the ones in the proposed update.

Wikipedia is not always an authoritative source, but it is a good indication of how terms and concepts are understood by the majority. This is particularly true where basic terms and concepts are concerned.

There are also some other definitions used in specific contexts. In general, it is common to see these two terms used synonymously.

[3] It is also important to get away from the common practice of referring to judgment and qualitative factors in cases where the proper term is guesswork in the absence of any objective data.

Reconsider the approach rather than add explanations

It is possible to find nuanced ways of explaining away the problems described above. Doing so may be appropriate in an academic paper but is not advisable in a practical guidance. We recommend a more direct approach that will better accomplish the overall goal of providing guidance on metrics and measurements using the Framework.

No suggestion to apply or endorse any existing methodology

We do not advocate that NIST replace or augment the approach to risk measurement and management in the proposed update with any of the existing methodologies or so-called standards. In cyber risk management, the best known of the existing approaches to have not been shown to provide an adequate picture of the risk, and can potentially lead to wrong decisions. They do not necessarily provide a foundation for additional, more detailed, risk treatment. NIST has made a wise decision in not to following or adopting any of these approaches.

Need for discussion and consultation on the technical issues

We invite NIST to get involved in further consultation to discuss additional details. These comments cannot be a substitute for in-depth technical explanations and discussions that should take place.

NEED FOR GUIDANCE ON THE DEFINITION OF CRITICAL INFRASTRUCTURE – TO WHOM DOES THE FRAMEWORK APPLY?

In the NIST Framework for Improving Critical Infrastructure Cybersecurity, critical infrastructure is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”[4]

[4] In 42 U.S.C. 5195c(e) - Critical infrastructures protection (“Critical Infrastructures Protection Act of 2001”), it is stated, “the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” The same definition is used in the Presidential Executive Order - Improving Critical Infrastructure Cybersecurity of Feb 12, 2013 (E.O. 13636, 2013, the Cybersecurity Enhancement Act of 2014 (S.1353) and elsewhere).

In the Executive Order 13010, as amended, it is stated “Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").” (E.O. No. 13010, July 15, 1996, 61 F.R. 37347, as amended by E.O. No. 13025, Nov. 13, 1996, 61 F.R. 58623; E.O. No. 13041, Apr. 3, 1997, 62 F.R. 17039; E.O. No. 13064, Oct. 11, 1997, 62 F.R. 53711; E.O. No. 13077, Mar. 10, 1998, 63 F.R. 12381; E.O. No. 13138, §3(c), Sept. 30, 1999, 64 F.R. 53880).

While we do not believe that the two definitions are different, it is possible to argue that they may be different if they have been used in slightly different contexts and for slightly different purposes. This would add to the possible confusion. Again, we believe that the definitions are identical, except that one of them further details specific sectors of the critical infrastructure.

The above definition perfectly captures the meaning of critical infrastructure. However, it does not—nor can it—provide a clear and unambiguous answer to the question of where the critical infrastructure ends and the "non-critical" infrastructure starts.

Industry sectors included in the critical infrastructure are specifically listed.[4] While this identification of the industry sectors is important, there is some confusion as to what enterprises within those sectors are part of the critical infrastructure.

Some appear to follow a very broad interpretation and believe that every enterprise within these sectors is part of the critical infrastructure. Others tend to prefer a more narrow interpretation and include in the critical infrastructure only the most important enterprises within these sectors. They point out that, for example, a small one-person insurance agency probably should not be classified as part of the critical infrastructure simply because it is part of the banking and finance sector. In the absence of guidance, it may be difficult to draw the line at the appropriate place.

Need for guidance on what enterprises are part of the critical infrastructure
To the degree possible, this guidance has to be provided. The situation of having numerous enterprises unsure whether the Framework applies to them is unacceptable.

While the Framework may be of use to enterprises outside of the critical infrastructure, there is a significant difference between knowing that the Framework directly applies to an enterprise, and seeing the framework as one of the many tools potentially helpful to the enterprise in improving its cybersecurity.

Question of the interpretation chosen by NIST
We understand that NIST may not see itself as the government agency best suited to provide proper interpretation of a term defined in the law. In this case, it will still be helpful to the cybersecurity community and other parties to gain better understanding of what interpretation NIST has used in the Framework development.

IMPORTANCE OF PREVENTING UNINTENDED CONSEQUENCES IN THE USE OF THE NIST CYBERSECURITY FRAMEWORK

The Framework has been developed for the critical infrastructure, with the additional consideration of facilitating wider adoption of the 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 any enterprises outside of critical infrastructure. The general foundation of the Framework is applicable to almost any enterprise. The Framework itself is not.

As an example of misuse or 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 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 it is done for enterprises for which the Framework has not been designed, potential results can be characterized as suboptimal at best.

It appears that the confusion exists even though the words “critical infrastructure” are in the very name of the Framework. We believe it would be helpful to state clearly that the Framework is designed only for enterprises that are part of the critical infrastructure. In addition to providing more clear guidance in the update to the Framework, it can be done through education of the industry.

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 the government agencies and the industry on issues related to the Framework and cybersecurity in general. We applaud the leadership of NIST in the area of advanced cybersecurity.

Sincerely,

Alex Krutov
President
Navigation Advisors LLC
www.navigationadvisors.com