October 8, 2014

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
(Attention: Ms. Diane Honeycutt)

Experience with the Framework for Improving Critical Infrastructure Cybersecurity
(79 Federal Register 50891 DN: 140721609-4609-01)

The Framework for Improving Critical Infrastructure Cybersecurity developed by NIST in close collaboration with other government agencies and the industry and released in February 2014, represents an important instrument for managing cybersecurity-related risks in critical infrastructure. It serves as and goes beyond being an effective approach to prioritizing and optimizing the tasks of following or developing guidelines, practices, and standards, to promote the protection of critical infrastructure.

The significant positive impact of the introduction of the Framework is undeniable. However, its full benefits have not yet been taken advantage of. In addition, some changes to and improvements of the Framework will be beneficial.

We limit our comments and suggestions to specific areas where we believe we can either (1) provide useful information relevant to the RFI or (2) offer a perspective potentially different from that of most other organizations. Our overall perspective is influenced in part by the actuarial and insurance views of risk in general and cyber risk in particular. *The focus on potential areas of improvement is not in any way indicative of a negative view of the Framework. In fact, we believe the introduction of the Framework to be a very important and necessary development*.

1. Our experience and interaction with other organizations have shown that the levels of knowledge of the Framework, as well as the process of its adoption, differ very significantly by industry sector and within the individual sectors we have been exposed to. This is understandable given that the process has only started and an initiative of this magnitude may take years to make a significant impact.

2. While the current levels of knowledge of the Framework are understandably low in most sectors, we already have a concern that in the longer term, the Framework may inadvertently be imposed on companies outside of the critical infrastructure. The Framework has never been intended to directly apply to such companies without adjustments.

   2.1. Enterprises in the critical infrastructure that deal with organizations that are not part of the critical infrastructure may start (and in some cases appear to have started) to require their vendors and other parties to follow the Framework. In the future, this can have a spiral effect and may ultimately affect the whole economy and its every sector. Without specific adjustments, the Framework should not be inadvertently imposed on organizations for which it is clearly inapplicable.

   2.2. Lack of understanding of the Framework and of the stated intention that it not become a mandatory standard, could lead to attempts to use the Framework as a checklist or as required best practices, effectively forcing its adoption where it may not provide the best solution. If insurance companies include specific questions about following the Framework in their applications for cyber insurance, an improper incentive to implement the Framework may be created. (At the same time, these questions and scrutiny by the insurance companies may in some cases have a positive effect. If lower insurance premiums are charged where cyber risk is lower, proper incentives are created.)

3. The voluntary nature of the Framework may need to be further emphasized. It appears that at least a small number of organizations have assumed that the Framework is mandatory for all practical purposes unless there are extremely compelling reasons to adopt a different approach. We do not believe this has been the intent of NIST. We also note the danger of the other extreme, that is, of not seriously considering the adoption of the Framework because of its voluntary nature.

4. Smaller businesses usually don't have the resources to implement or understand the Framework. This is a significant concern. While the lack of resources to implement standards or best practices may often be addressed by using outsourcing or consulting arrangements, the lack of expertise to understand best practices or standards presents a greater problem. Outsourcing without understanding creates its own risks of potential significance.

   4.1. It may be argued that small and medium size businesses without such expertise should not be active participants in the critical infrastructure industries. While this logic is understandable, it amounts to a policy decision made in an indirect way,

potentially resulting in significant realignment in specific sectors and a reduced number of smaller businesses.

4.2. It would be particularly troubling if smaller businesses outside of the critical infrastructure are affected in a negative way and lose contracts to bigger organizations. To address this concern, modifications to the Framework may be warranted to create versions better suited for organizations outside of the critical infrastructure area.

5. We have observed some confusion as to where the Framework should applied or is recommended to be considered for adoption. We believe it will be beneficial if additional clarification is communicated to clearly define (a) where the Framework should be considered for adoption, while emphasizing its voluntary nature, and (b) what organizations are part of the critical infrastructure.

6. While the Framework references and includes the definition of critical infrastructure, there is often confusion where the line between the critical and non-critical infrastructure actually lies. For example, while the financial sector is part of the critical infrastructure, not every organization within the financial sector is part of the critical infrastructure. This clarity is needed and should be communicated.

To answer some of the specific questions in the RFI not addressed above, we can also add the following:

- The Framework has helped some organizations to better understand the importance of managing cyber risk. Their number is growing. However, at this point the main factor is not the details of the Framework content but rather its very existence.

- The Framework may benefit from better covering and incorporating advances in authentication solutions. This is an area where the risk level is very high but promising solutions to its reduction are being rapidly developed.

- We have done some limited work to help educate others about the Framework and are considering expanding greater efforts on this activity.

- There is a need to develop measures of conformity assessment in both the private and public sectors.

- We are concerned with the possibility of the NIST Framework or its elements becoming parts of compliance checklists. While compliance is a critical element of cybersecurity,

there is danger of defaulting to the general checklist mentality in practical implementation. This danger would exist even where a different framework is adopted.

- We believe that many organizations have limited expertise in quantifying cyber risk. Consequently, they may incorrectly prioritize the necessary cybersecurity activities and measures. This is a broad issue that the Framework helps to address or at least bring attention to. However, we believe that more could be done in the area of risk quantification. Our expertise in the analysis of insurance risk (including in the context of risk analysis for cyber insurance pricing) and analytics leads us to believe that significant progress can and should be made in cyber risk quantification. The NIST Cybersecurity Framework can facilitate this progress.

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.

Alex Krutov
President
Navigation Advisors LLC
www.navigationadvisors.com

Alex.Krutov@NavigationAdvisors.com
1.646.361.3255