https://NavigationAdvisors.com

February 9, 2016

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

Re: Views on the 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 information on its Cybersecurity Framework.[1]

These comments and suggestions are limited 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 of 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 Framework is an increasingly important part of cyber risk management.

RELATIVE VALUE OF DIFFERENT PARTS OF THE FRAMEWORK, MOST USEFUL PARTS OF THE FRAMEWORK, AND AREAS FOR POTENTIAL IMPROVEMENT

- We believe that the primary value of the Framework is in its broad unifying approach and not in any of its parts considered on their own. The value of any particular element is often sector-specific and also specific to an organization within a sector.

- Regarding your question about the extent of risk reduction due to the Framework (i.e., measurable benefits of the Framework):

  — Observations of cybersecurity practices at a number of organizations, as well as of data breaches and other cyber failures, lead us to conclude that the risk reduction and the very adoption of the Framework or its elements differ very significantly from organization to organization. Some organizations have derived clear benefits from

[1] Please note that these comments are not intended to represent the views of the CAS Task Force on Cyber Risk chaired by Alex Krutov and are not provided on its behalf.

using the Framework while others still have not used the Framework and have limited understanding of it.

— Measuring the extent to which the Framework has reduced an organization's cybersecurity risk and specific metrics used is **an area where the Framework may be further improved and additional guidance provided**.

— This area involves **analytics**, a dimension **significantly lagging in cyber risk management**. Few organizations use **meaningful quantifiable measures** of cyber risk that would permit the analysis of risk reduction or finding proper tradeoffs among various risk management options. Any additional guidance that can be provided or incorporated in the Framework will be beneficial.[2]

- Assessment of the preparedness and cyber risk levels by individual enterprises is absolutely necessary. However, another type of assessment, crucial in the context of critical infrastructure protection, involves looking at the bigger picture and taking into account interdependencies among the enterprises, in order to assess the overall risk to the critical infrastructure and understand the best ways to manage this risk and to prioritize cybersecurity activities.

  — While this function lies with the government and not any individual enterprise, the usefulness of the Framework will be enhanced if the need for this general assessment is clearly considered in the Cybersecurity Framework and guidelines for its implementation.

  — Some standardized outputs of cyber risk analysis would be useful in this context. Increased voluntary information sharing may also help in achieving this goal. (This comment is not meant to suggest changing the voluntary nature of the Framework.)

LONGER TERM GOVERNANCE OF THE FRAMEWORK AND POSSIBLE DIRECTIONS OF FUTURE DEVELOPMENTS

In regard to specific questions NIST is seeking to answer, we can state that

- **NIST should not transition the coordination of any elements of the Cybersecurity Framework to another organization.** Unless the intent is to change the nature of the Framework, **splitting the "ownership" of the Cybersecurity Framework may have**

[2] Significant research has been conducted in this field since the introduction of the Framework. We have developed certain expertise in this area, focusing on the use of probabilistic frameworks in cyber risk assessment, and can share some of the research conclusions. Important research in this area has also been done by a number of organizations including NIST itself.

significant negative consequences for the national security and critical infrastructure protection.[3]

— A single agency should be in charge of the overall coordination. This agency should have the expertise and hold full responsibility for the maintenance and future development of the Framework.

— If another agency assumes this responsibility, it would have to be taking over the whole Framework and not simply some of its elements. At this point, we believe that NIST is the right organization to manage the Framework. NIST has tremendous expertise in this area. While additional expertise is needed, NIST should have the ability to build some of this expertise internally and also get access to additional expertise from other sources.

— NIST should take advantage of the resources of other agencies and the private sector. The strength of the Framework is based, to a significant degree, on the numerous inputs that NIST has been able to incorporate or consider in its development. Future developments would benefit from the same approach.

— Some agencies may have specific expertise that would be of particular importance in any future changes of or additions to the Framework. This deep expertise not found elsewhere should continue to be utilized by NIST, and in some cases the input from these parties should have an even greater weight in any future changes or developments. This coordination will also prevent the development of parallel frameworks which, while similar to the NIST Cybersecurity Framework, would be in a number of ways duplicative; it would be preferable to add modifications of the NIST Framework necessary to account for specific cybersecurity threats, vulnerabilities or objectives.

— We also believe that NIST has the advantage of having developed the 800-series special publications that document many of the standards and practices. At the same time, we suggest that the overview of the publications be considered in order to

- assure consistency among the publications themselves and their usefulness to organizations implementing the Framework
- make updates, if any are necessary, to account for the developing cyber landscape
- eliminate, if possible, parallel standards for different organizations except where these differences are clearly justified[4]

[3] We believe that the critical need for active involvement of the DHS in all areas that involve protection of the critical infrastructure does not require any comments.

[4] An example would be aligning practical FISMA implementation with the Framework and the main NIST publications in some areas if it is considered feasible and appropriate.

- Sector-specific coordination of the Framework's **actual implementation, and providing specific guidance on some elements of the implementation, should be a joint effort of NIST and other agencies**. We do not suggest any changes in this area but rather, even closer cooperation. The private sector plays an important role in this process.

- We encourage the use of international standards. At the same time, we caution against their overly broad use, without careful consideration, in protecting the critical infrastructure.[5]

  — We support the use of international standards and welcome their adoption. Some of them are broadly used and are important in addressing cybersecurity threats.

  — International standards are growing in importance as the economy is becoming more global. Compliance with different but largely duplicative standards creates an additional burden on enterprises operating in more than one country and can put these enterprises at a competitive disadvantage.

  — We emphasize the importance of monitoring the "more critical" part of the critical infrastructure[6] where the use of international standards not under control of the U.S. government[5] may not be the optimal way to protect the U.S. critical infrastructure.

- Consistent with the requirements set out in EO 13636, making any changes to the Cybersecurity Framework should be done in a way that assures the inclusion of methodologies to identify and mitigate impacts of the Framework and associated measures or controls on business confidentiality, and to protect individual privacy and civil liberties.[7]

OTHER

- **Further education is necessary to prevent unintentional misuse of the NIST Cybersecurity Framework**

  — The Framework should not be imposed on enterprises for which it has not been designed. It has been developed only for critical infrastructure, which already represents a significant slice of the private sector. Its use by other enterprises may be suboptimal.

---

[5] In some cases, such standards can be modified in suboptimal ways by the standard-setting bodies, or they may not be modified in a timely manner when changes are necessary. This creates a potential national security concern. At the very least, it is important to be very closely involved in the work of the standard-setting bodies and have the willingness to adopt different sets of standards if appropriate.

[6] This is not necessarily synonymous with the "critical infrastructure at greatest risk" as defined in the Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11742.

[7] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11741.

- Additional education is needed to prevent the possibility of wrong incentives for adopting the Cybersecurity Framework. One example would be an insurance company offering cyber insurance and asking, as part of the underwriting process, whether the enterprise considering the purchase of cyber insurance follows the NIST Framework. Where this question is asked of companies that are not part of the critical infrastructure, it may create the impression that following the Framework is expected; it may even create an incentive to follow the Framework in order to reduce insurance premiums. This may lead to some enterprises deciding, for the wrong reasons, to adopt the Framework which has not been developed for them.

- We also consider it important to revisit the question of incentives for enterprises in the private sector to adopt the Cybersecurity Framework. This includes but is not limited to the issues of (a) cyber insurance and (b) data sharing.

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.

Sincerely,

Alex Krutov
President
Navigation Advisors LLC
www.navigationadvisors.com

Alex.Krutov@NavigationAdvisors.com
1.646.361.3255