MITRE

13 December 2013
H120-L-014

National Institute of Standards and Technology
Information Technology Laboratory
ATTN: Adam Sedgewick
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Subject: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

MITRE's comments on the Preliminary Cybersecurity Framework are enclosed. Our comments discuss the purpose of the Framework, the voluntary nature of Framework adoption, and the Framework's implicit organizational rather than holistic view of industry. The comments also recommend more emphasis on resiliency, consideration of a threat-based defense approach, more about privacy, additional definitions, and changes to some of the security control mappings.

We support your efforts to make the Cybersecurity Framework even more useful in helping to reduce the cybersecurity risk to the Nation's critical infrastructure. Please let us know if you have any questions. Thank you.

Sincerely,

Bradley Schoener

Bradley Schoener, Ph.D.
Portfolio Manager, National Economic Infrastructure

Enclosure

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102-7539

MITRE Summary Comments on NIST Preliminary Cybersecurity Framework

- **Framework Purpose**. The functions defined in the Framework Core (Identify, Protect, Detect, Respond, and Recover) are focused on identifying and sharing threat information, while many of the activities in the subcategories, especially in the Identify and Protect functions, are related to establishing a cybersecurity program within an organization.
    - For clarity, we recommend the Framework document focus on managing and communicating cybersecurity risk. Recommend moving guidance on how to establish a cybersecurity program to an appendix, or reference other sources and state as an assumption that organizations have already established a cybersecurity program.
    - In addition, Executive Order (E.O.) 13636 indicates that DHS, OMB, DOD, and other organizations will provide additional services and intelligence. Recommend referencing these other efforts that are identified in the E.O. and describing how they fit within the Framework.
- **Voluntary Nature of Framework**. Recommend incorporating information related to the incentives programs from the Departments of Treasury, Commerce, and Homeland Security into the Framework to fulfill the objective of *encouraging* organizations to *consider cybersecurity risk*. There is also limited information in the Framework to address a *cost-effective*, *performance-based* approach as called for in E.O. 13636.
- **Holistic View of Industry/Sector Framework**. Individual organizations face cybersecurity risk within the context of their broader industry/sector ecosystem. Recommend moving the Framework beyond its current focus on securing individual organizations to address the cybersecurity challenges of industries/sectors as a whole.
    - Recommend adding a function to the Framework, *Orient*, that identifies the need for each organization to define its place within the ecosystem in relationship to other organizations in an industry/sector. While many of the potential subcategories applicable to this function are included in other existing functions, consolidating them in a new function, *Orient*, focuses attention on the concept of framing an organization's cybersecurity posture within its much larger industry/sector ecosystem.
    - In the Introduction, include *Orient* and briefly discuss the concept that organizations exist as part of an industry/sector ecosystem, the value of sharing information within the ecosystem, and threat-sharing roles and responsibilities.
- **Resiliency**. Resilience addresses the needs of an organization that enable it to continue to operate, possibly in a degraded state while maintaining mission essential functions, after an adversary breaches the organization's defenses. While the need to "strengthen the resiliency of this infrastructure" is recognized, recommend adding specific subcategories to address resiliency, for example add a function to the Framework, *Withstand*, that identifies the needs of an organization to adapt to evolving threats and continue fulfilling mission essential functions during periods of degradation that affect an organization's own operations and that of their external stakeholders. Potential *Withstand* categories could include: a) Prepare: maintain a set of cyber courses of action that address predicted cyber-attacks; b) Prevent: preclude successful execution of an

attack on a set of cyber resources; c) Continue: maximize the duration and viability of essential mission/business functions during an attack; and d) Constrain: limit damage from an adversary's attack. The Respond and Recover functions currently do not address these resiliency concepts.

- **Threat-based Defense**. A threat-based approach to protecting the critical infrastructure provides a proactive rather than a reactive approach to managing cybersecurity risks, providing the opportunity to make intelligence-driven decisions.
    - In order to address cyber threat intelligence, an organization needs to identify potential targets (people, information, systems, etc.), identify likely adversaries who will seek to go after these targets, learn how these adversaries operate, figure out if/how networks are appropriately implemented to collect data to capture/halt these adversaries, adjust corporate policies and architectures to support adversary observation, containment, and more.
    - To be more effective, most of the threat data gathered for analysis is not an incident but rather data from earlier in the intrusion lifecycle (also called the "kill chain"); these earlier events might include, for example, spear phishing attempts, googling, public website trolling, etc.
    - Recommend discussing the threat-based defense concept in the Introduction and have cyber threat intelligence drive execution of the core functions. Explain how the information is pulled into the organization's cyber threat knowledgebase, correlated with/against existing threat and log data, and used to make intelligence-driven decisions.
    - Broaden the Respond function, in keeping with an overall threat-driven approach, to specifically address how cyber event data is captured and then folded into the cyber threat analysis process.
- **Scope of Privacy and Civil Liberties Methodology**. The privacy and civil liberties discussion blends general organizational privacy requirements (e.g., provide notice, limit use) with privacy considerations that are specific to cybersecurity (e.g., dispose of personally identifiable information, manage privacy and civil liberty concerns during incident containment).
    - Recommend including more discussion regarding private sector privacy requirements and standards to better draw the link between the Fair Information Practice Principles (FIPPs), NIST SP 800-53 Appendix J references, and the applicability of the content in the framework's Appendix B to cybersecurity activities.
    - Recommend focusing the guidance on identifying and managing privacy risks, especially those beyond basic compliance. This guidance will help organizations allocate their resources appropriately and better protect PII when addressing cybersecurity.
- **Definitions**. Recommend adding definitions for *cybersecurity*, *risk tolerance*, *outcome*, *ecosystem*, and *sector*.