October 10, 2014

VIA EMAIL: cyberframework@nist.gov

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

RE: Experience with the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

The American Insurance Association (AIA)\(^1\) welcomes the opportunity to provide feedback regarding industry experience with the Cybersecurity Framework (Framework). Overall, AIA and its members have a very positive reaction to the Cybersecurity Framework and the process by which it was developed. While it is still too early to truly understand the Framework’s impact, we generally feel it serves as a flexible tool that identifies general concepts in a common risk management process. We did not individually answer each of the questions identified in the Request for Information (RFI), but instead provide thoughts for your consideration on the broad themes emerging from the questions.

**Awareness**

We firmly believe that there is an awareness of the Framework; however, the level of awareness varies among industries. Naturally, those owners and operators of critical infrastructure as well as highly regulated industries may, by their very nature, be more security oriented and as such are likely to have a working understanding of the Framework. On the other hand, there are entities that may simply know the Framework exists and do not realize how it could be useful. For this reason, it might be advantageous to explore ways for the Critical Infrastructure Cyber Community C\(^3\) Voluntary Program to gain more traction in the press as resource for more than just critical infrastructure operators.

---

\(^1\) AIA represents approximately 300 major U.S. insurance companies that provide all lines of property-casualty insurance to U.S. consumers and businesses, writing nearly $100 billion annually in premiums.
**Cyber Insurance**

The awareness of the Framework combined with headline stories about data breaches has stimulated an interest in cyber insurance. As the cyber insurance market grows insurers continue to explore ways to meet increasing market demands. There is a competitive market and ultimately each individual insurer will choose how, if at all, it will incorporate the Framework into its underwriting practices. However, generally the Framework presents an interesting opportunity to assist in understanding how thoroughly a customer has contemplated their cyber risks and data standards. Further, we believe that the Framework establishes a useful common lexicon for communicating with customers when engaging in the underwriting process. While it remains too early to assess the effectiveness of the Framework and its impact on underwriting practices, we continue to monitor and assess its progress.

**Insurance Industry Experience**

Generally, we feel positively about the NIST Framework. The overall concept of the framework and the fact that it is mapped to already-existing standards is very useful. In particular, we appreciate that the Framework has four different tiers, which is good from a 'maturity' perspective. Different companies will have different maturity levels based on various factors including, but not limited to: size, industry, and risk tolerance. The Framework is also assisting companies to stay focused and on-track when reviewing their risk management strategies.

**Success**

Importantly, the Framework was built to allow continued use of other risk management strategies. Therefore, incorporation of the Framework into these existing strategies is a good indicator that the Framework is successful; however, it is important to keep in mind that the opposite is not necessarily true. The lack of incorporation of the Framework into a corporate risk management strategy does not serve as a good measure of the Framework’s success. A company’s review and consideration of the Framework relative to existing risk management strategies, in and of itself, is a success of the Framework, because it means companies are taking the time to assess their organizations capabilities to “identify, protect, detect, respond, and recover.” However, at times, an entity’s existing risk management structure may be more robust.

In addition, the Framework strikes the appropriate balance between guidance and flexibility, which allows a company to weigh internal business risks. As such, we question whether the Framework can be specific enough so that companies are able to measure their own compliance against the Framework’s standards. Therefore, the cost associated with compliance may be high for some entities, particularly those that would look to a third-party to assess compliance or are already ISO compliant.

For these reasons, the success of the Framework should not be based on the lack of incorporation as it cannot be the sole basis for judging cyber hygiene and resiliency. This concept is key to recognizing the significant value in the voluntary nature of the Framework.
**Roadmap for the Future of the Cybersecurity Framework (Roadmap)**

We look forward to continuing to work with NIST as they move forward on collaborating with the private sector to address on-going challenges related to cybersecurity. Of particular interest is real-time threat indicator sharing. We encourage Congress to pass a meaningful information-sharing bill that will provide companies with timely and actionable information. We would also prioritize “Federal Agency Cybersecurity Alignment,” “Cybersecurity Workforce,” and “Supply Chain Risk Management” as important issues identified in the Roadmap. Further, we would encourage continued focus on educating the C-Suite and Board of Directors regarding the usefulness of the framework, and their corporate and personal liability regarding information security.

Thank you for the opportunity to provide comment and we look forward to working with you on the important issue of data security. We are happy to answer any questions that you may have.

Respectfully submitted,

Angela Gleason  
Associate Counsel