AMERICAN INSURANCE ASSOCIATION

2101 L Street NW
Suite 400
Washington, DC 20037
202-828-7100
Fax 202-293-1219
www.aiadc.org

December 13, 2013

VIA EMAIL csfcomments@nist.gov

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

RE: Preliminary Cybersecurity Framework

Dear Mr. Sedgewick:

The American Insurance Association (AIA)[1] appreciates the opportunity to provide comments on the Preliminary Cybersecurity Framework. We commend the National Institute of Standards and Technology (NIST) for their diligent and thoughtful development of the Cybersecurity Framework (Framework). Overall the Framework, as currently drafted, is a well-constructed flexible document that is easy to comprehend and aligns with existing standards such as COBIT and ISO, which many companies have already adopted.

Information is a key element to the business of insurance and as an industry we appreciate the significant responsibility we have to maintain its privacy and security while balancing practical day-to-day business applications. As such companies have been developing internal cybersecurity best practices since the 1980's to protect consumer data, and corporate networks and systems. These best practices are developed based on risk assessments of anticipated and existing threats, a company's size and risk profile, and the ever-evolving landscape of technological solutions. Therefore, the insurance industry has many mature systems in place to accommodate the business need and robust state and federal legislative and regulatory structure that we are subject to. It is with this background that we provide some constructive comments for your consideration below.

[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.

Profiles and Tiers

We have concerns that the Profiles and Tiers are not sufficiently described to encourage continuous improvement of security practices. For instance, there is not enough information to clearly differentiate the maturity levels between what is described as Tier 3 vs. Tier 4. Too much is left open to subjective interpretation that could result in companies describing their program as a Tier 4 when in reality their maturity level is something less.

In addition, many existing frameworks will assess the design and effectiveness of controls at the sub-category level and then use these lower level assessments to roll-up a composite maturity rating. This type of approach seems to be missing from the Framework. Instead the Tiers are defined at a higher aggregate level. Such a sub-category approach may assist with promoting continuous improvements in security practices.

Conformity Assessments

Appendix C identifies areas of improvement that should be addressed through future collaboration, including conformity assessments. It is unclear what role these conformity assessments will play and how they are to be conducted. There is a serious concern that a government requirement for a conformity assessment could lead to significant unplanned costs should an independent or external auditor be required to assess corporate security programs.

Privacy and Civil Liberties

As drafted, the methodology to protect privacy and civil liberties contained in Appendix B is overly prescriptive and may conflict with existing corporate best practices or legal requirements. For example, page 29 directs companies to retain PII for as long as is necessary and permitted to fulfill the specified purpose." However, corporate best practices surrounding record retention may require information to be retained for other purposes such as potential litigation. Also, the broad-based principles in current Appendix d not have an obvious connection to the Framework and are therefore overreaching.

As an alternative, we support the substance of the "Methodology to Protect Privacy for a Cybersecurity Program" established in the letter from Harriet Pearson of Hogan and Lovells. This alternative approach recommended by Hogan and Lovells is clear and straightforward and recognizes the applicability of existing standards, best practices, and legal requirements. Further, it continues the theme of flexibility as championed in the Framework. We recommend that NIST eliminate the existing Appendix B and incorporate the Hogan and Lovells' proposed privacy methodology.

Cost

The Framework as currently drafted generally appears to be an inclusive and not disruptive document for those with mature systems currently in place, but it may be too early to say this with certainty. While it ultimately remains to be seen, there should be minimal costs related to implementing the Framework for companies with existing mature systems. However, this may not be the case for a less mature company that will experience initial up-front costs.

Adoption

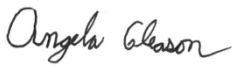
We echo the comments that have been expressed by many that there needs to be a clear understanding of what constitutes adoption of the Framework. NIST has committed a significant amount of effort to develop the Framework and now it is important to understand what adoption of the Framework looks like. Any definition of "adoption" should reflect the voluntary nature of the Framework as contemplated by Executive Order 13636 and NIST and should not be prescriptive.

****

Overall, the Framework strikes the appropriate balance between guidance and flexibility, allowing companies to weigh internal business risk when determining how to effectively implement the framework. If widely adopted, the Framework has a number of potential benefits including: (1) creating a foundation that provides executive level read-out reports with enough low-level direction to understanding and communicating the requirements for implementation; (2) establishing a common language to: (a) describe security practices when requested by customers, audits, etc.; and (b) to better communicate with consumers when they are purchasing cybersecurity insurance; (3) leveraging the information profiled and provided to a company by its partners; and (4) integration into existing 3rd party assessment processes.

There is potential value to the Cybersecurity Framework and we look forward to working with you as you move toward a final version of the Framework as well as future editions. Thank you for the opportunity to provide comment and we are happy to answer any questions that you may have.

Respectfully submitted,



Angela Gleason
Associate Counsel