AMERICAN INSURANCE ASSOCIATION

555 12th Street NW
Suite 550
Washington, DC 20004
202-828-7100
Fax 202-293-1219
www.aiadc.org

September 9, 2016

Commission on Enhancing National Cybersecurity
National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Via Electronic Mail to cybercommission@nist.gov

Re: Cyber Insurance

Dear Members of the Commission on Enhancing National Cybersecurity:

The American Insurance Association (AIA) appreciates the opportunity to respond to your Request for Information (RFI) as published in the Federal Register, Volume 81, No. 154 on August 10, 2016. AIA is the leading property-casualty insurance trade organization, representing approximately 325 major U.S. and non-U.S. insurers that write more than $127 billion in premium each year and provide all lines of property-casualty insurance to consumers and businesses. Of significance to this RFI, many AIA members are significantly involved in the cyber insurance market and as such have an interest in the Commission on Enhancing National Cybersecurity's (Commission) curiosity in cyber insurance.

The RFI seeks information as to the current and future challenges; approaches to address those challenges; and recommendations on ten identified topics to include cyber insurance. Below we provide background on the cyber insurance market, challenges to the growth of this market and recommendations for your consideration. Overall, AIA notes that the cyber insurance market should be allowed to evolve organically and any government intervention should be carefully scrutinized to avoid stifling innovation and the growth of this beneficial product. We respectfully encourage the Commission to consider this when outlining its recommendations.

Background

The product that is typically referred to as "cyber insurance," more often referred to as Network Security and Privacy Insurance by insurers, dates back approximately 15 years with its origins in technology errors and omission insurance. This insurance product provides coverage for financial losses that resulted from negligent acts, errors, and omissions in the deliverance of technology products and services. In 2002, California enacted the first state data security breach notification law, which became the starting place for the current patchwork of laws in 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands. This resulted in costs previously not contemplated by Insureds for the forensic activities necessary to identify which consumers were impacted, legal fees associated with determining how best to comply with each state or territory's notification rules, and the costs of actual mailings and offering of credit monitoring services. As such, "cyber insurance" as a stand-alone product evolved and today may include both liability-type coverages as well as "first-party coverage" for the Insured's own losses.

More specifically, first party coverage is insurance that applies to the Insured's own property or personal losses, whereas third party insurance covers an Insured's potential liability to third parties. For instance a cyber event may include a denial of service attack, destruction of data whether through malware or human error, system failures, cyber extortion threats, a breach of personal information, etc. If such event triggers "first party coverage" the policy may provide payment for loss experienced directly by the Insured such as notification, investigation and public relation expenses as well as losses occasioned by business interruption, theft, and equipment or data restoration. The "third party coverage," on the other hand, would include costs associated with damages and expenses incurred in connection with claims brought against the Insured by third parties such as costs associated with responding to or defending against regulatory inquiries, payment of fines, and lawsuit liability.

The above examples of cyber events and coverage are only examples and will of course depend on the actual insurance policy, as issued. As with any specialized insurance product, cyber insurance is best understood in the context of the type of risks presented by our digital world and the way in which insurance seeks to address risk, generally. An insurance policy typically covers a particular type of loss (e.g. property damage), often without regards to the cause of the loss, with certain exceptions and exclusions. As such, there are in fact many types of policies that "cover" losses caused by a network security event, without specifically being a "cyber insurance policy" per se. Network security threats are a relatively new risk not necessarily contemplated by traditional insurance lines and coverage for these cyber perils, but as these types of losses become more pervasive and the risk more fully understood, insurance carriers are creating tailored polices, endorsements, and restrictions for cyber related losses.

Cyber should be considered a peril and coverage for the cyber peril can be addressed, in whole or part, in a dedicated, stand-alone product or embedded in a multi-risk policy that might include cyber as one of the many causes of loss, for instance a commercial property policy or a directors and officers' policy. The decision on how best to address a given entity's cyber risk is typically made with the advice of an insurance agent or broker whose expertise guides the Insured in evaluating its coverage needs and existing insurance products to determine whether insurance gaps exist and how to best address those gaps. For example, a commercial general liability policy is generally not intended to cover data breach event; an Insured should be aware that a stand-alone cyber liability policy should be considered to provide that coverage.

Underwriting Process

As suggested above, a typical commercial insurance purchase process involves a consultation with an entity's insurance agent or broker to understand the client's business, likely including its general exposure to cyber security losses. A part of this process, the broker will provide a broad range of information about the client to the insurance carrier(s) from whom coverage may be sought. Typically, this information is submitted in the form of a basic insurance application and, as applicable, specialty questionnaires to better assess the risk the client poses and how that fits into the insurer's risk appetite. Factors such as the size of the company, industry, risk management efforts, and the type of coverage sought will determine whether further information, including conference calls or in-person meetings with the company's information security personnel, counsel, or management, would be beneficial to the underwriting process. Cyber insurance underwriters often wish to have an understanding of the applicant's contractors, vendor arrangements and the company's and vendor's approach to data protection, internal cyber practices/policies, and past events. For example, the insurer may wish to know whether there is a written risk management program, does the company require employee training, are policies updated with predictable frequency, what kind of personal information does the company collect, does the company inventory its software and IT assets, have there been any cyber events, and what kind of controls are in place to respond to an incident. In addition, some insurers may use an accepted information security standard, such as the NIST Framework, as a communication tool when talking with applicants. Essentially, the insurer needs a general understanding of an entity's cyber risk and how it approaches network security, in part to determine whether information security risk awareness is incorporated into the corporate culture and how it views the potential for liability.

Cyber Insurance's Role

As with many other emerging and complex risks, insurance is a valuable tool in crafting a risk management program. First and foremost, it is a useful targeted risk transfer mechanism. The application process can also be a resource to companies as they think through their own individual risk assessments. Unquestionably, though cyber insurance is but one aspect of a far broader solution to increasing our nation's cyber resiliency. Creating greater cyber resiliency is a societal obligation achievable with the involvement of both the public and private sectors, as a whole, coming together to share information and best practices to manage this growing and evolving risk.

Cyber insurance, while an important risk transfer product, should not be seen as a driver of behavior or guarantor of cyber security. To be sure, risk analysis is a meaningful aspect of the underwriting process and the insurance relationship. However, insurance cannot, and should not, be considered a standard-setting vehicle to drive better behavior thereby increasing the nation's cyber resiliency. Cybersecurity requires an ever-evolving adaptable approach that is incorporated into an entity's overall risk culture and each individual company is uniquely and best able to assess its own risk and global approach to managing cyber exposures. For these reasons, assuming a check-the-box approach in which buying insurance assures a total solution to cyber risk or as a complete risk assessment tool would be a grave miscalculation of how this dynamic threat should be managed.

The benefit of thinking through risk portfolios is a significant by-product of the insurance underwriting process, but insurance alone should not be looked at as a tool to change behavior. Further, competitive considerations in the insurance market – including a dynamic of new capital entrants – have yielded extremely varied risk appetites and underwriting procedures, such that a company may be able to procure cyber insurance without the corresponding improvements to its cyber security posture.

Challenges to Market Growth

The cyber insurance market continues to grow responsibly and remains committed to addressing the various challenges to continued growth, including the following:

- Education – Businesses are not always convinced that they are at risk of a cyber event.

- Data and Risk Modeling – The risks presented by the cyber age are new and more rapidly evolving compared to more traditional risks that insures have been underwriting for hundreds of years. Thus, sufficient loss data and risk modeling capabilities, which are critical to responsible underwriting, will need time to develop. Moreover, the risk is continually evolving as bad actors look for new ways to expropriate information and process it for their own purposes.

- Aggregation and Accumulation – As indicated above, coverage for cyber events may be embedded in a number of insurance policy types. Further, cyber is also a global challenge, sometimes without geographic borders or predictable locational centers, thereby increasing the geographic risks broadly. The increasingly interconnected business environment and the ubiquitous presence of cyber in our commercial world also serves to increase the aggregation and accumulation risks insurers must manage.

Forensic Reports

A lack of actuarial data is not the only data gap that insurers may face. Often times Insureds may avoid sharing data such as forensic reports with their insurer in an effort to avoid an assertion that they have waived the attorney client or work product privilege. Though these concerns are understandable, failing to provide forensic information hurts insurance carriers and their clients in two ways: (i) it makes it more difficult to evaluate claims triggered by a cyber event given that critical information is withheld from the carrier; and (ii) there will be less information available to insurance carriers to aid in risk management and risk transfer solutions for the client and more broadly for the benefit of the cyber insurance market. A healthy flow of information to insurance carriers that underwrite cyber risks helps to facilitate the availability of loss mitigation tools and products to the public. Moreover, the free flow of accurate information concerning cyber risks and events can help support underwriting and claims handling, which in turn will assist in building a robust and sustainable cyber insurance market.

Legislators can help play a role here by creating an exemption from the waiver of attorney client or work product privilege when policyholders share forensic data with their insurer.

Allow the Market to Grow

As with any emerging insurance market it takes time to develop data points and model risks. For that reason, many insurers are investing significant time and resources to gain the necessary data and modeling experience to enable broader cyber coverage and greater capacity. In this regard, we strongly caution against the suggestion that a standardized policy form would serve the market well. At this nascent stage of development, insurance options should not be stifled or constrained by standardization, which might only serve to limit the innovation and product offerings that insurers are developing to meet the needs of our clients and the ever evolving and dynamic nature of the information security risks. In addition, similar to a company's decisions to manage cyber risk, insurers must also determine their risk tolerance, particularly given the aggregation and accumulation concerns outlined above. Standardization could push a carrier to avoid certain risks that it may otherwise have been willing to consider if not pushed into a standard policy form or policy language. Moreover, with

such a rapidly changing risk as this, the development of a standard form that would be responsive to buyers' needs and achieve market-wide acceptance might be impossible. If appropriate, standardization will evolve as the market evolves. Lastly, Insureds are not left to fend for themselves in evaluating and choosing cyber coverages – they quite fortunately have a large universe of capable, well-versed insurance agents and brokers available to guide the buyer in analyzing the available products and capabilities of the participants in the cyber insurance market.

As we have highlighted throughout this response, AIA and its members strongly believe that the scope and size of a business' cyber insurance purchase should be carefully analyzed and reviewed with a qualified cyber insurance broker. The selection of a product and an insurer as well as the role of insurance in the management of cyber risk should remain with the business. As a key partner in cyber security, government should rightly encourage conversations about the role of risk transfer and cyber insurance in managing cybersecurity, but should be extremely wary of any approach suggesting a mandated offer, scope, or form of cyber insurance. Allowing the market to develop at a responsible pace, over time, will enable a healthy evolution of the role of insurance in the larger cyber ecosystem.

* * *

Cyber insurance is a valuable risk transfer mechanism that often serves as a useful tool to help companies think through their cyber risk exposures. However, it is important to note that insurance is not and should not be considered the driving force to changing behavior or ensuring adherence to government-developed standards. Businesses and their advisers are in the best position to evaluate their risk management approach, including insurance needs; we believe that the market will evolve and continue to grow to meet the increasing consumer demands. Thank you again for your attention to this matter and for the opportunity to comment on the role of insurance in enhancing the nation's cyber preparedness.

Respectfully submitted,

Angela Gleason
Counsel