AMERICAN INSURANCE ASSOCIATION

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

April 29, 2013

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Via Electronic Mail to cyberincentives@ntia.doc.gov

Re: Incentives to Adopt Improved Cybersecurity Practices

Dear Sir or Madam:

The American Insurance Association (AIA) appreciates the opportunity to comment on potential incentives to promote the adoption of the Cybersecurity Framework (Framework). AIA is the leading property-casualty insurance trade organization, representing approximately 300 insurers that write nearly $100 billion in U.S. premium each year. Our members offer a variety of property-casualty insurance, including personal and commercial auto insurance, commercial property and liability coverage for businesses, homeowners' insurance, workers compensation, product liability insurance, and medical malpractice coverage. The notice of inquiry seeks information on the benefits and relative effectiveness of potential incentives, including liability insurance. Briefly, we do not believe that liability insurance should be considered a tool to incentivize companies to adopt the Framework. Instead, we believe attention should be given to: (1) developing standards that are consistent with existing requirements; (2) bolstering education; (3) encouraging frequent software updates; (4) increasing training; and (5) promoting liability protections for information sharing.

Liability Insurance

There is a market for cyber liability coverage and we need to allow the market to work. In developing the Framework, the National Institute of Standards and Technology (NIST) states that its mission is to promote U.S innovation and industrial competitiveness. Cyber liability coverage is one area where this mission can be accomplished. For example, companies will continue to refine their existing products or create new ones in response to existing market conditions and the risks the market can tolerate. Education and increased awareness of cyber threats will inevitably increase knowledge about the liability products available to assist in developing one's risk management portfolio. Just as cybersecurity cannot be a one-size-fits-all approach, neither can a cyber liability policy. Both cybersecurity and cyber liability coverage require a risk-based approach based on individual company assessments.

Insurers writing cyber liability coverage continue to educate themselves to understand and advance their underwriting capabilities. Continued advancements in the cyber insurance market will depend on access to sufficient loss data and a knowledgeable workforce that stays current with changing technologies and threats. A well-crafted Framework that encourages education and allows for information sharing will support the development of the cyber insurance market.

However, conversely, we seriously question how insurance could incentivize the adoption of a framework of standards, methodologies, procedures and policies that are undeveloped and have not been proven or even tested as an effective solution to cyber threats.

In addition, the Terrorism Risk Insurance Act (TRIA) treats cyber-terrorism, for availability purposes, just like any other risk of loss. If an insurance policy would provide coverage for cyber–losses, however caused, coverage for cyber-terrorism would be offered. If the policy generally excluded cyber-losses, the insurer would be under no obligation to make cyber-terrorism coverage available and it would otherwise be excluded from the policy. The underwriting characteristics of terrorism loss make it different from other types of loss and difficult, if not impossible, to insure without the public-private shared loss program under TRIA. Thus, any consideration of incenting solutions through insurance must factor in both the existence and stabilizing nature of TRIA, as well as the realities of the insurance marketplace with respect to certain types of cyber-risk.

Consistency

One of the fundamental elements to promoting the adoption of the Framework by critical infrastructure and the broader business community is to develop standards that build upon existing laws, standards, and best practices. New and inconsistent requirements will inevitably create confusion and inadequate protections that ultimately dissuade voluntary adoption.

Education

Education will also be a key component to promoting the adoption of the Framework. The federal government should engage in an educational campaign that not only increases awareness of the Framework but also highlights the benefits of adoption. Given the sensitive nature of this issue it is clear that a detailed campaign is not possible; however, a campaign that highlights examples of the impact a cyber-attack has on a company either through first-hand accounts or a centralized location for articles, can have a big impact on small businesses that may not have the man-power to devote the time to following this issue. Further, the educational campaign should focus on how the standards can achieve good cyber hygiene.

Software Updates

As noted at NIST's Cybersecurity Framework Workshop on April 3rd, good cyber hygiene is one of the three key elements of any cybersecurity program. A primary component of cyber hygiene is keeping pace with the evolving nature of cyber risks and solutions. Most system exploits result from a company's use of back versions of software because they have failed to keep their security patches up-to-date. Keeping software and operating systems up-to date should be an integral part of all risk management portfolios.

As many small business and end customers purchase services rather than build program codes, the best practices should focus on providers of service, i.e. cloud service providers, software providers, and hardware manufacturers and incentivize them to build-in minimum standards and easily executed update schedules.

Training/Certification

Currently there is a shortage of IT professionals with necessary skill sets in the area of IT security. Moreover, there is a failure among existing professionals to keep their skills up to date. A program that encourages growth of IT security skills and competencies is another effective program that the government should consider. This could include a certification process for IT professionals.

Similarly, the government could establish a certification process for companies similar to the Payment Card Industry Data Security Standard (PCI DSS) certification. This certification would allow companies to publicize that they have met certain minimum security standard requirements.

Further, in AIA's letter to NIST, we identified existing commonly adopted standards recommended by leading security organizations and standard setting organizations including the International Organization for Standardization's (ISO) 27001 standard. In fact, many commentators at the April 3rd Workshop also pointed to ISO standards. To the extent the Framework builds upon and references these standards, a grant program that

supplements costs for ISO certification would be a beneficial and cost effective incentive. This would be cost effective not only for small business, but also in terms of avoiding creating and staffing a certification program from the ground up.

Information Sharing

We support the efforts of the federal government to create a voluntary network of cyber threat information sharing among private sector entities and between the private sector and government. The success of such a program will depend on federal legislation that establishes liability protections and limits information sharing to the technical nature of the threats and avoids the sharing of personal or commercially-sensitive information. In addition, legislation will also need to consider antitrust protections.

As noted above, the sharing of actual loss information among insurers and with the government could assist in continued maturation of the cyber insurance market and allow for a more consistent, predictable and sustainable insurance environment.

* * *

Fundamentally, the key to incentivizing adoption of the Framework, and in fact promoting good cyber hygiene generally, will require a multilevel approach focused on education, training, affordability and consistency with existing laws. Thank you again for your attention to this matter. Cybersecurity is an extremely important issue that our members take very seriously and we look forward to working with you.

Respectfully,

Angela Gleason
Associate Counsel