AMERICAN INSURANCE ASSOCIATION

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

April 8, 2013

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

Via Electronic Mail to cyberframework@nist.gov

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

The American Insurance Association (AIA)[1] appreciates the opportunity to comment on the development of a framework to reduce cyber risks to the critical infrastructure ("Cybersecurity Framework"). The National Institute of Standards and Technology's (NIST) Request for Information (RFI) notes that the "Cybersecurity Framework" will not only assist those identified as critical infrastructure, but also interested entities.[2] AIA's members place significant importance on the protection of their data, networks, and systems. In addition, our industry is currently subject to a robust legislative and regulatory framework at both the state and federal level. Therefore, we provide the following information to assist NIST as it begins to develop the Cybersecurity Framework.

Use of Frameworks, Standards, Guidelines, and Best Practices

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. 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. An offensive and defensive strategy employs strong counter measures that not only defend against existing threats, but also attempt to anticipate and deter potential threats.

Companies use a variety of resources from the insurance industry and broader financial services sector, to develop best practices. Generally, this could include standards recommended by leading security organizations, industry groups, multi-sector sharing forums, vendors, third party consultants, and other professional associations. For example, the International Organization for Standardization (ISO) 27001 standard or even NIST's own S.P. 800-53 are standards commonly referenced.

[1] AIA is the leading property-casualty insurance trade organization, representing approximately 300 insurers that write nearly $100 billion in 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.

[2] "Cybersecurity Framework will provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties."

When adopting security practices and programs companies may build the program in-house or purchase a product from service providers. Careful attention is placed on selecting the appropriate security products that implement the guidelines and best practices identified during a company's risk analysis. A service provider that establishes robust standards as part of its standard offering is extremely beneficial.

Furthermore, these best practices or standards cannot remain static. Companies continuously monitor, review, and refine their best practices and standards to address new threats and technologies. This includes insuring that the software and hardware programs are up-to-date and running the latest versions.

Specific Industry Practices

In establishing best practices and standards, the industry is also guided by an extensive yet flexible structure of statutes and regulations. Examples of statutes, regulations, and standards include but are not limited to:

Gramm Leach Bliley Act (GLBA)

Section 501(b) of GLBA requires state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards: (1) to insure security and confidentiality of customer records and information; (2) to protect against anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer. Regulators have long held that this means a written and effective information security program.

State Insurance Privacy Laws

The National Association of Insurance Commissioner's (NAIC) developed a model regulation that requires insurers to implement a comprehensive written information security program that includes administrative, technical and physical safeguards to protect customer information. At least 35 states have adopted regulations designed in accordance with this model. In addition, the NAIC has developed the following model laws for adoption by individual states: Insurance Information and Privacy Protection Model Act and Privacy of Consumer Financial and Health Information Regulation.

Market Conduct and Financial Condition Examinations

As part of the state-based regulatory structure that governs insurance companies, state insurance departments may conduct a review of company practices. To assist state examiners in this process, the NAIC developed the Market Regulation Handbook and Financial Examiner Handbook. Both of these handbooks provide a flexible approach for examiners to evaluate internal company standards and computer controls. In addition, examiners are required to provide for the security of company records and information.

State Data Breach Laws

These laws encourage entities that maintain an individual's personal information to have adequate security in place, including methods of encryption, to protect personal information. As of August 2012, 46 states, DC, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

State Privacy Laws

Several states require entities that store an individual's personal information implement specific data and security standards. For instance, Massachusetts Regulation 201 CMR 17.00 (Standards for the Protection of Personal Information of Residents of the Commonwealth), requires entities that store or have access to the data of Massachusetts residents to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluate and improve, where necessary, the effectiveness of the current safeguards of limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.

Regulation S-P

The U.S. Securities and Exchange Commission (SEC) adopted regulations S-P privacy rules promulgated under Section 504 of the GLB Act. It requires the investment companies, broker-dealers, and investment advisors to have administrative physical and technical safeguards in place to protect customer information. Additionally, these rules require financial institutions to provide their customers with notice of their privacy policies and practices. These financial organizations are prohibited from disclosing private personal information about a consumer to nonaffiliated third parties, unless the institution provides certain information to the consumer and the consumer does not elect to opt out of disclosure.

Securities and Exchange Commission (SEC) Corporate Finance Disclosure Guidance

The SEC's Corporate Finance Division ensures that investors are provided with material information in order to make informed investment decisions, both when a company initially offers its securities to the public and on an ongoing basis as it continues to give information to the marketplace. In October of 2011, the SEC's Division of Corporate Finance issued topic #2 pertaining to its views regarding disclosure obligations relating to cybersecurity risks and cyber incidents. These disclosures include risk factors, legal proceedings, financial disclosures and others.

Payment Card Industry (PCI) Standards

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PADSS), and PIN Transaction Security (PTS) requirements. These standards require companies that store credit card data to have certain information security protocols in place to protect this data. In addition, PCI Standards require an annual assessment of these protocols by a third party.

* * *

Cybersecurity is an extremely important issue that our members take very seriously. Given the sensitive and complex nature of the issue, we hope that this general overview of the extensive framework our companies are influenced by is beneficial. We would be pleased to arrange a meeting of our cybersecurity experts, should you be interested in discussing this matter with greater detail.

Thank you again for your attention to this matter and we look forward to working with you.

Respectfully,

Angela Gleason

Angela Gleason
Associate Counsel