AMERICAN INSURANCE ASSOCIATION

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

February 23, 2016

VIA EMAIL: cyberframework@nist.gov

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

**RE: Views on the Framework for Improving Critical Infrastructure**

Dear Ms. Honeycutt:

The American Insurance Association (AIA)[1] appreciates the opportunity to provide feedback on the "Framework for Improving Critical Infrastructure" (Framework). While we are not critical infrastructure for the purpose of the Framework, our members overall have found value in the Framework as a flexible benchmarking and communication tool. 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. The responses below are from the perspective of our internal corporate use; however, we would note that insurers continue to monitor and assess the progress and success of the Framework. Each insurer will choose how, if at all, it will incorporate the Framework into its underwriting practices now and for the future, but at a baseline we feel that the common lexicon creates a useful tool for communicating with our insureds and perspective insureds.

The organization and common lexicon presented in the Framework not only enable insurers to communicate more effectively with their clients, but it also enables our information security professionals to effectively communicate with C-suite and internal management. The common lexicon created by the Framework is one of its key assets.

The RFI requests information on how to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes." It is our view that there could be value in the National Institute of Standards and Technology (NIST) developing a voluntary standard process/program for performing a Tier Assessment for the Framework, which could be utilized by regulators as well as external and internal auditors that perform risk assessments of an information security program. Such a process or program may help with any conflicting and duplicative regulatory processes and regulatory requirements that exist.

[1] AIA represents approximately 325 major U.S. insurance companies that provide all lines of property-casualty insurance to U.S. consumers and businesses, writing nearly $117 billion annually in premiums.

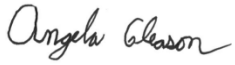
In addition, at this time, AIA does not believe there is a need to update the Framework; however, it should be regularly reviewed to keep pace with the constantly emerging cyber threats and challenges that arise. We strongly believe that the principles that guided the initial development of the framework should continue with any update to the Framework. As such the same successful public private partnership process should be utilized and the Framework should remain flexible, voluntary and build upon the current Framework and existing standards.

Further, NIST should not transition the Framework's coordination to another organization. Nevertheless, if NIST were to consider a transition, the depth, breadth and history of the organization should be considered to ensure the long term sustainability of the Framework. As such the ISACs may be a viable option. In addition, NIST should ensure that there would be no impact to the current usage of the Framework; however, if transitioned and changes are proposed, a roadmap should be developed to describe how to get from the current state to a proposed future state.

Finally, we do see value in the continued socialization of the Framework and the potential benefits of using it. We suggest that one potential venue for socializing the Framework could be at Information Sharing and Analysis Center (ISAC) Summits.

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