NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

Local Agents Serving Main Street America℠

April 8, 2015

Commissioner Adam Hamm, Chair
C/O Pam Simpson
NAIC Cybersecurity (EX) Task Force
444 N. Capitol Street NW, Suite 700
Washington, DC 20001

***VIA EMAIL: psimpson@naic.org***

Dear Commissioner Hamm,

On behalf of National Association of Professional Insurance Agents (PIA)[1], I would like to thank the NAIC for focusing on the important issues around managing cyber risk, cybersecurity, and associated insurance products and to offer comments on the proposed "Principles for Effective Cyber Security Insurance Regulatory Guidance" (Principles). PIA supports the efforts of the NAIC to ensure that insurers and insurance producers have robust cybersecurity and risk mitigation programs. In addition, PIA supports efforts by the NAIC to help foster a strong cyber insurance market; as we believe that cyber insurance products are integral to the economic security and stability of the U.S.

In general, PIA agrees that there must be a consistent and coordinated national approach to cybersecurity, highlighting cooperation between states and the federal government. PIA also appreciates the Principles' recognition that any approach must be "flexible, scalable, practical, and consistent" and that a "one-size-fits-all" approach to cybersecurity will not be sufficiently effective. Finally, PIA believes that the Principles should be enduring and not overly rigid. Please see below PIA's specific comments on Principles 5, 6, 12, 14, and 15.

**Principle 5**
Principle 5 references the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is an important standard for managing risk, but it is not the only standard. Many other standards and procedures, beyond NIST, may be more appropriate tools for insurance producers. Further, as technology changes, best practices for managing cyber risks are likely to evolve. PIA suggests language such as, "… and other similar, current, and future standards for managing cyber risks" be added to the end of Principle 5.

[1] PIA is a national trade association founded in 1931 which represents member insurance agents in all 50 states, Puerto Rico, Guam, and the District of Columbia. PIA members are small business owners and insurance professionals who can be found across America. Furthermore, PIA members, in numerous states, currently sell cyber liability insurance products through a PIA sponsored program.

NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

Local Agents Serving Main Street America℠

**Principle 6**
PIA supports Principle 6 and commends the NAIC for including it. PIA members are small and mid-sized business owners. As such, very different risk mitigation programs are necessarily utilized by PIA member agents and agencies than in large corporations. PIA believes that the resources, size, nature of business, and the risk-profile of insurance producers are all essential considerations when establishing regulatory guidance on cybersecurity.

**Principle 12**
PIA agrees that cybersecurity risks should be included and addressed as part of an insurance producer's enterprise risk management processes. However, regulators should, in line with Principle 6, consider that internal risk management processes will vary based on the resources, size, nature of business, and the risk-profile of insurance producers in any oversight on this issue.

**Principle 14**
PIA agrees that sharing information and staying informed about cyber and physical threat intelligence is necessary. But, requiring membership in one specific group may actually undermine this goal. The FS-ISAC is an excellent organization, but it is specially tailored for financial services. There are other Information Sharing and Analysis Centers (ISACs) and methods that may be more appropriate for insurance producers. PIA asks for more flexibility in this principle and suggests language such as, "Insurers and insurance producers should stay informed about cyber and physical threat intelligence analysis and sharing, which may be accomplished by joining an ISAC."

**Principle 15**
PIA agrees that sensitive data collected, stored, and transferred inside or outside of an insurance producer's network should be protected, and encryption is one way to do that. However, encryption is only one way to protect data based on current technology. PIA recommends that this principle be less prescriptive as to the precise method to be used to achieve appropriate data protection. Instead, PIA suggests removing the word "encrypted" and inserting "appropriately safeguarded."

PIA appreciates the considerable effort that has gone into drafting these principles, and we are grateful for the opportunity to provide the independent agent perspective on these important issues. Please contact me at jennwe@pianet.org or (703) 518-1344 with any questions or concerns. Thank you for your time and consideration.

Kind Regards,

Jennifer M. Webb, Esq.
Counsel & Director of Regulatory Affairs
National Association of Professional Insurance Agents