Draft: March 12, 2015

Principles for Effective Cybersecurity Insurance Regulatory Guidance[1]

Due to ever increasing cybersecurity issues, it has become clear that it is vital for insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. The insurance regulators commend insurance companies for conducting a review of their cybersecurity policies, regulations, and guidance with the goal of strengthening the insurance sector's defense and response to cyber-attacks. The insurance industry looks to the insurance regulators to aid in the identification of uniform standards, promoting accountability across the entire insurance sector, and to provide access to essential information. The insurance regulators also depend upon the insurance industry to join forces in identifying risks and the offering of practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers and the insurance industry.

Principle 1: Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks.

Principle 2 Insurance regulators have a significant role and responsibility regarding the insurers' efforts to protect sensitive customer health and financial information.

Principle 3: Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC.

Principle 4: Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.

Principle 5: Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 6: Regulatory guidance must consider the resources of the insurer or insurance producer.

Principle 7: Effective cybersecurity guidance must be risk-based and threat-informed.

Principle 8: Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 9: Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

Principle 10: The effective management of cybersecurity by third parties and service providers is essential for protection of consumer's sensitive personal health and financial information.

[1] These principles have been derived from SIFMAs (Securities Industry and Financial Markets Association) "Principles for Effective Cybersecurity Regulatory Guidance"

Principle 11 Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information.

Principle 12 Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.

Principle 13 High level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.

Principle 14 It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.

Principle 15 Sensitive data collected and stored and transferred inside or outside of an insurers or insurance producers network should be encrypted.

Principle 16 Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.

Principle 17 Enhanced solvency oversight is needed for insurers selling cyber insurance to businesses and families.

Principle 18 Additional data on the sale of cyber insurance products should be collected to assist insurance regulators with oversight of financial and market regulation.