Memo

To:	Adam Hamm, Chair, NAIC Cybersecurity (EX) Task Force
cc:	Patrick McNaughton, Chair, NAIC IT Examination Working Group
From:	LeeAnne Creevy and Philip McMurray, RRC
Date:	March 23, 2015
Subject:	RRC Response to the NAIC Cybersecurity (EX) Task Force Regarding the Draft List of "Principles for Effective Cybersecurity Insurance Regulatory Guidance"

Background

On March 12, 2015, the National Association of Insurance Commissioners ("NAIC") exposed two cybersecurity-related exposure drafts for comment. The first of these exposure drafts included a set of 18 principles designed to "help state insurance departments identify uniform standards, promote accountability, and provide access to essential information". As an interested party, Risk & Regulatory Consulting LLC ("RRC") offers comments related to several of the principles included in the exposure draft, with the full scope of our response aligned with the principles referenced below.

In parallel with this response, RRC has also actively supported the NAIC's IT Examination Working Group ("ITEWG"), including recent efforts focused on enhancing the assessment of cybersecurity risks during the financial examination process. RRC provided a response to the ITEWG's request for input regarding cybersecurity risks and examination testing in February of this year, and we are currently volunteering to help align the NAIC IT review guidance with cybersecurity standards published by the National Institute of Standards and Technology ("NIST"). We fully support the efforts of the NAIC Cybersecurity Task Force and the ITEWG to enhance regulatory guidance regarding cybersecurity risks.

We appreciate the opportunity to offer our comments. Please note that we have elected to not comment on the exposure draft principles that are not referenced below as we concur with their content.

Comments Regarding Specific Principles

RRC's comments appear below, referencing specific principles both individually and grouped where appropriate.

> **Principles 5 and 6** – Recognizing the need for a scalable approach for performing regulatory examinations, RRC concurs with these principles with the caveat that a minimum set of cybersecurity standards be in place for all insurers that are physically connected to the Internet or other public data networks, regardless of size and scope of operations. Given the current ITEWG initiative to align the IT review process with existing NIST guidance, the practical definition of what constitutes this minimum standard can, and should, be included in the ITEWG's efforts. However, because the Cybersecurity Task Force's principles will serve to help guide those efforts, Principle 5 and/or Principle 6 should include language stating that a minimum set of cybersecurity standards should be defined for all insurers that make use of public data networks.

Principles 8, 12 and 13 – Transcending the IT review process, these three principles focus on the need for a holistic, top-down view of cybersecurity risks. While RRC fully agrees with these principles, it is also imperative that the financial examination process be extended beyond current ITEWG-based initiatives to include expanded procedures regarding executive-level cybersecurity awareness, inclusion of cybersecurity risks within the insurer's ERM process and integration of cybersecurity into organizational strategic planning efforts. As a result, these principles should either be expanded, or they should be directly supported by extensions to the current financial examination guidance (for example, expanding guidance in Exhibit Y of the Examiners' Handbook related to C-level management interviews), thereby mirroring the current ITEWG initiatives that are focused on IT-related controls and processes.

Principles 11 and 14 – RRC fully agrees with these principles, with the understanding that active information sharing among insurers and other financial services entities can significantly improve a shared understanding of cyber threats, and an enhanced ability to respond in a timely and effective manner. RRC also recommends that current wording of these principles be extended to encourage participation in other current and future information sharing forums. For example, Principle 14 references a significant information sharing group (FSISAC). However, a number of other cyber-threat sharing forums exist or are planned, including the one proposed at the White House Summit on Cybersecurity and Consumer Protection in February, 2015. As such, we recommend that consideration be given to broadening Principle 14 to include more than just the FSISAC.

Principle 15 – This principle addresses an important consideration relative to protection of insurer data, both in-transit and at-rest. However, RRC recommends that additional specificity be added relative to the definition of "sensitive". The wording of the currently-drafted principle is somewhat ambiguous, allowing for interpretation of this term by insurers and entities that provide services to the industry. RRC recommends that existing data classification methods be referenced by this principle, with possible choices including the current NIST 800-60 and FIPS 199 guidance. It was also noted that this term is used in Principles 2, 3, 10 and 11, and RRC encourages a clearer definition of this term to help ensure consistent and appropriate data protection efforts are undertaken.