August 3, 2015

Patrick McNaughton
Chair
IT Examination Working Group
National Association of Insurance Commissioners (NAIC)
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

By email to Miguel Romero at maromero@naic.org

RE: CYBERSECURITY-RELATED REVISIONS TO PROCEDURES USED BY REGULATORS IN THE EXAMINATION OF INSURANCE COMPANIES – Comments on the Proposal to Make Revisions to the Handbook Guidance

Dear Mr. McNaughton:

Below are comments on the exposed proposal to make cybersecurity-related revisions to the guidance provided to regulators performing examinations of insurance companies. Please note that some of them summarize, without going into detail, a few of the points I made on the June conference call of the working group. We hope that you will find these observations and recommendations useful.

Addressing Cyber Risk in Regulatory Oversight

We fully support your work on incorporating cybersecurity-specific guidance in the standard procedures used in the examinations of insurance companies. The growth of cyber risk exposure of insurance companies has been dramatic and is expected to continue. It is important to make sure that examiners have specific guidance related to cybersecurity.

While the need for specific guidance is evident, we also support your intent to maintain the flexibility needed to account for significant differences in cyber risk exposure and potential ways to manage cyber risk that may exist between two seemingly similar insurance companies. This flexibility is also important in light of the evolving nature of cyber risk and the danger to putting in place overly rigid guidance that may quickly become outdated.

"Cybersecurity Considerations"

The "Cybersecurity Considerations" addition to the General Information Technology Review section of the Financial Condition Examiners Handbook outlines key elements of cyber risk management by insurance companies that regulators are expected to examine.

1. *General Framework* We support the non-prescriptive general nature of the framework described in very broad terms. There are a number of frameworks for assessing and managing cyber risk. With the exception of cases where there are specific regulatory requirements, it would be inappropriate to endorse and effectively mandate the use of one particular formal framework.

2. *Expected Level of Cyber Risk* As the term is used in the first paragraph of the section, "exposure to cybersecurity risks" appears to refer to the general exposure, before taking into account reduction to the risk due to implementation of risk controls, proper policies, etc. Based on that definition, in the current environment we should assume that an insurance company has "significant exposure to cybersecurity risks" as defined. Not having this level of exposure is likely to be an exception and not the rule. The language used is not entirely clear and may appear to be contrary to this observation.

3. *NIST Cybersecurity Framework* The names of the four elements presented in the description (Identify, Prevent, Detect, and Respond & Recover) are very similar to the names of the five Core Functions of the NIST Framework for Improving Critical Infrastructure Cybersecurity (Identify, Protect, Detect, Respond, and Recover). While the description and even the number of elements are different, some may interpret the current language as a direct reference to the NIST Framework and possibly a recommendation that it be adopted. We want to bring this to your attention but do not make a recommendation on whether the general language should be changed.

4. *Identifying Cyber Risk Exposure* The proposal refers to reviewing "insurer's risk mitigation strategies and/or controls that identify, prevent and detect cybersecurity incidents." This is inconsistent with the text that immediately follows, where "identify" is specifically explained as a reference to identifying cyber risks, that is, identifying exposure to potential cyber-related events as opposed to identifying actual incidents. This is also inconsistent with the general logic of the rest of the same paragraph. We suggest that the language be changed to have "identify" refer to identification of cyber risk and better understanding of ways it can be managed.

5. *Participation in Information Sharing Networks* Description of the "identify" element includes a statement that "participation in information sharing networks is crucial for organizations to understand constantly evolving risks." We would like to point out that participation in such networks is at least equally important in the "prevent" and "detect" elements as they are defined in the proposed guidance. Furthermore, we are concerned that "participation in information sharing networks" is likely to be interpreted as sharing (providing) information. While there is a strong argument that such information sharing would have strong benefits to the industry as a whole, it is not necessarily "crucial" for an individual company to share its information in order to "understand constantly evolving risks." Even where participation in the so-called information sharing networks does not require providing information, it cannot be called "crucial" because there may be other ways to obtain cyber risk information relevant to a specific company.

6. *Planning for Contingencies* The description of the "respond & recover" element includes the language that says, "When incidents do occur, it is important that the insurer performs a thorough post-remediation analysis and that the insurer understands how it will restore services that were affected as a result of the incident." We suggest that the sentence be reworded to make it clear that

understanding of how to restore services is required to be established in the planning process and not "when the incidents do occur."

7. *Service Providers and Other Third Parties* A service provider may expose an insurance company to significant cyber risk if this exposure is not properly managed. This is appropriately emphasized in the proposal. However, the reference to legal agreements with service providers includes only examples that have to do with financial indemnification. The biggest component of the risk may not be directly indemnifiable, such as the risk of suffering significant reputational damage. For this reason, it is critical that the actual agreements directly require third parties to maintain appropriate cybersecurity procedures.

8. *Mergers & Acquisitions* We are glad to see that the proposed addition emphasizes the need to examine recently acquired or integrated companies more carefully. These situations can present a very high level of cyber risk.

9. *Engaging Cybersecurity Experts* The proposal also says, "To the extent that the examiner determines that the insurer does not have proper procedures to identify, prevent, detect, respond, and recover from cybersecurity incidents, the examiner may consider incorporating the use of a cybersecurity expert in IT procedures performed." We assume this statement references engaging cybersecurity consultants for the purpose of confirming the examiner's conclusions or developing recommendations. If this understanding is correct, we suggest that the language be changed to include the situations where the examiner has not made a negative determination. The examiners should be easily able to engage experts even at earlier stages of the examination, when no conclusions have been reached. Engaging such experts should be seen as a reflection on the competence level of the examiner. Many examiners do require training in cybersecurity. However, there are also situations where cyber risks are quite complex and engaging a cybersecurity expert is the only way to perform the examination properly.

Information on Breaches Involving Confidential Information

The Information Technology Planning Questionnaire contains proposed addition labeled Information Technology Security – Incident Response. This section requires providing a listing of "any instances in which confidential information may have been breached" and asks for extremely detailed information about every such instance.

1. *Definition of Breaches Involving Confidential Information* We believe that the current definition is not sufficiently clear and may in some case be unnecessarily broad. "May have been breached" is not sufficiently precise to provide clear guidance. We note that the more definitive "was breached" is used in the same description later. Much more problematic is the definition of confidential information. Some companies use very broad definitions of confidential information. Other companies use narrow definitions of confidential information.

2. *Level of Detail* The level of detail about broadly defined breaches involving confidential information is such that many companies may be unable to provide all of the required data. This may include even companies that manage their cyber risk much better than the current industry norm.

Need to Avoid Increase in Cyber Risk Due to Potential Breach of Government or NAIC Systems

The examinations involve collecting some very detailed sensitive information on insurance companies' systems and data. This information can make it much easier for hackers to launch a successful cyber attack against insurance companies. Storage of the information on servers of state insurance departments opens the possibility of hackers gaining access to the data by penetrating these systems. Aggregating this information means that a single point of failure can results in the compromise of data affecting many insurance companies. If there is any use of the NAIC systems, we have to consider the possibility that these systems can be breached too. Collecting information of highly sensitive nature creates natural targets for hackers.

If the information is held on the systems of consultants engaged to provide assistance to examiners, there is an additional risk that their systems can be breached, creating additional failure points.

We share with you these observations in order to make sure the issue is carefully considered and addressed. We do not question the need to collect and analyze data in order to examine whether cyber risk is properly managed by insurance companies.

Please note that these comments and recommendations represent my personal views and are not intended to reflect the position of the P/C Risk-Based Capital Committee of the American Academy of Actuaries, which I chaired until approximately a year ago, or the CAS Task Force on Cyber Risk, which I currently chair. These personal views should not be seen as a public policy statement, nor as a position taken by any of these two organizations.

Sincerely,

Alex Krutov, FCAS, ASA, MAAA, CERA
President
Navigation Advisors LLC
alex.krutov@navigationadvisors.com
www.navigationadvisors.com