September 8, 2015

Patrick McNaughton
Chair, ITEWG
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: Additional Comments on the Proposed Cybersecurity-Related Revisions to Procedures Used by Regulators in the Examination of Insurance Companies

Dear Mr. McNaughton:

Below are comments on the revised proposal that calls for making cybersecurity-related revisions to the guidance provided to regulators performing examinations of insurance companies. While some of the comments are similar to those we have shared with you earlier, others are new. We hope that you will find the comments useful in finalizing the proposal.

Thank you for the attention your group has paid to our previous comments and for making some changes to the first version of the proposal to reflect our recommendations.

Importance of Addressing Cyber Risk in Regulatory Oversight

We *reiterate our strong support of your work* on incorporating cybersecurity-specific guidance in the procedures used by regulators 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 regulators have specific guidance related to cybersecurity.

"*Massive Data Breach*" of the Systems Maintained by the NAIC or by State Regulators Should Not Be the Next Headline: Avoiding Unintended Increase in Cyber Risk

The examinations involve collecting 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 result 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 a 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 extra risk that their systems can be breached, creating additional failure points. In addition, insider risk is always a concern.

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. We also understand that you are aware of the general concern and that other groups at the NAIC would need to be involved in making sure the regulatory examination process does not result in unintended increase in cyber risk.

Need for Integrative Approach to Cybersecurity in Enterprise Risk Management and the Responsibilities of the Senior Management and Members of the Board of Directors

Like you, we believe that cybersecurity is not a purely technical IT issue. Cybersecurity affects many areas of company operations and requires joint efforts by many professionals. It also requires involvement of the senior management and the Board of Directors.

Consequently, we suggest modifying or partially deleting the recently added language about the roles of senior management and the Board of Directors in the general section of the "Cybersecurity Considerations" draft. The relatively short section devotes disproportional amount of space to explaining that the examiner "should take into account the distinction between the roles of the insurer's Board of Directors and its senior management." The current language may lead to the general impression that the document is introducing and emphasizing an unusually restrictive role segregation between the management and the Board of Directors, with the ultimate result being the reduced responsibilities of the members of the Board of Directors. Such an impression should not be created because directors have crucial oversight responsibility. Since documents of this nature often become de facto industry standards that define overall expectations, it can even be seen as creating an additional legal defense for members of the Board of Directors in cases of alleged negligence leading to cybersecurity failures.

It may also appear to a reader that the changes to the draft attempt to de-emphasize, in general, the roles and responsibilities of the Board of Directors and to a lesser degree of the

senior management. Statements that the risk assessment process includes "some amount of management/board involvement, appropriate to the distinct roles of the board and senior management" may contribute to creating this impression. In reality, in creating proper risk culture and risk controls, the importance of the roles of the management and directors, distinct as they are, cannot be overstated. The repeated references to the "distinct roles" of the management and board (in this section and elsewhere) raise questions as to why this issue is being emphasized to such a degree. Regardless of the factual correctness of the statements, the excessive emphasis on this issue can be seen as strange in a document so short that it does not touch on many important aspects of cybersecurity. The roles of the Board of Directors and senior management are absolutely critical; these individuals bear the responsibility for everything the company does or neglects to do. This is always understood to be part of the proper corporate governance that takes into account both direct operational, general management, policy-setting, oversight and other interrelated roles.

Because risk governance is not limited to IT cybersecurity processes and systems, it may make sense to have closer interaction between the IT examiners and other regulators on the team. The current draft adds the following question to the list of sample questions for the CEO and the corresponding list for members of the Board of Directors (or its committee): "How does the company monitor, assess, and respond to information security risks (including those related to cybersecurity threats)?" We agree with the importance of adding this question. However, we are unclear on whether adding it to the questionnaires means that IT examiners or other regulators with technical cybersecurity expertise will now be part of the actual interview process (assuming the process is a face-to-face interview).

Information on Breaches Involving Confidential Information

The Information Technology Planning Questionnaire contains a 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. "Was or was likely to have been breached" is not sufficiently precise to provide clear guidance. Without definition of a breach, it is difficult to determine whether a data breach has actually happened. We note that data breach notification laws in place in most states do not provide a consistent definition of a breach. In some state laws, the term is not used at all. Equally problematic is the definition of confidential information. It is not always clear what constitutes confidential company information. The draft also refers to confidential policyholder information. This term has no standard definition. Where the policyholder is an individual, the term appears to be broader than the typical personal

information governed by state breach notification laws or federal regulations such as HIPAA.

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.

Cybersecurity is Not Only about Data Breaches

The never-ending announcements of data breaches have led to the general tendency to think of cybersecurity as protecting sensitive information. In reality, there are also other types of cyber failures. The focus on protecting sensitive information is perfectly appropriate as long as other potential cyber failures are not neglected. In some places, the current language of the draft creates the impression that protecting sensitive information is the only goal of cybersecurity. For example, the language added to the first paragraph of the "Cybersecurity Considerations" section (probably at the suggestion of an interested party) specifically refers to ways that are most appropriate for an insurance company to "most effectively protect its sensitive information." Considered together with the next sentence, this language may create an impression that the cybersecurity function is limited to protecting sensitive information.

Other Recommendations and Specific Suggestions

Below we list selected additional recommendations. Most of them are focused on clarifying the language of the draft.

In the first paragraph of the "Cybersecurity Considerations" section, the latest draft has the word "and" deleted. We believe this is an unintentional mistake that creates ambiguity. Later in the same paragraph, we suggest that the language "complexity of an insurer" be replaced with "complexity of insurer's operations." However, the reference to insurer's size earlier in the sentence is appropriate, which means that rephrasing the whole sentence may present the best option. The same sentence refers to "security laws and regulations." While the intent appears to be clear, we recommend that the word "security" be deleted in order to avoid any possible misunderstanding. The laws and regulations dealing with cybersecurity and breach notification requirements are generally not referred to as security laws and regulations. The term security regulations is typically used in a different context. The same paragraph refers to policies, systems and "framework or frameworks" that are "most appropriate for a particular insurer to most effectively protect its sensitive information." We suggest that "most appropriate" be replaced with "appropriate." The reason for making this suggestion is the

desire to avoid the impression that the use of the best (in a particular situation) framework or set of policies is required. The choice of the best or "most appropriate" may include a significant judgment component. While it is always the goal to choose the best approach and the most appropriate solution, regulatory oversight is intended to focus on adequate and effective as opposed to the very best. For the same reason, it may also make sense to delete the word "most" in "to most effectively protect" in the same sentence.

The description of the Respond & Recover element of cybersecurity policy or framework states that when a cybersecurity incident occurs and services need to be restored, it is important that they be restored in accordance with the response plan. We suggest that the words "in accordance with the response plan" be deleted. While it is always best to have an effective response plan for any situation, we know that in reality it may not be possible. In some cases, blindly following a pre-arranged routine can be a serious mistake. In cases where a response plan is very general and fits almost every situation, the statement is simply unnecessary.

The Information Technology Security – Incident Response section of ITPQ contains the list of information to be provided when confidential data may have been exposed. Leaving aside the previously made comment about the difficulty or impossibility of providing all of the information as well as the limited utility of some of it, we believe that the terms used require additional clarification. For example, the new draft references confidential policyholder information. We do not believe this is a clearly defined term. Data breach notification laws in place in almost every state generally use other terminology. We also note that the words "corporate governance" have been correctly deleted from the item asking to describe the extent of the involvement in data breach incidents by the senior management. We suggest that the deleted words be replaced with "and members of the Board of Directors" as appears to have been the original intent of the drafters of the first version. It is generally expected that in cases of serious data breaches, members of the Board of Directors or its committee would have some involvement as part of their risk oversight and general oversight responsibility. Another line item mentions "legal claims to be incurred" as part of the breach costs. This term is unclear and confusing. If the reference is to the expected costs associated with lawsuits and the expected figure is known, then the expenses have probably already been "incurred" under both statutory and GAAP accounting rules. On the other hand, if the figure can't be estimated, then it can't be provided. We also want to point out the difficulty of estimating these costs as we have observed in litigation related to large data breaches at non-insurance enterprises. The utility of always requiring that this information be provided is somewhat limited even though in most cases it is best to obtain all available information.

Additional Comment

We strongly support your work and believe that the cybersecurity-related revisions you are making are going to be an important part of assuring proper management of cyber risk by insurance companies. Even though the comments above suggest certain changes and potential improvements, the proposal itself is solid and put together in a very competent manner.

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
President
Navigation Advisors LLC
alex.krutov@navigationadvisors.com
www.navigationadvisors.com

cc: Adam Hamm, Chair of the NAIC Cybersecurity Task Force
Eric Nordman, Director of the NAIC Center for Insurance Policy & Research
Tony Cotto, NAIC Financial Policy and Legislation Counsel
Aaron Brandenburg, NAIC Economist and Statistical Information Manager