VI A E MA IL

March 23, 2015

Mr. Adam Hamm, Chair
Cybersecurity (EX) Task Force
National Association of Insurance Commissioners
2301 McGee Street, Suite 800
Kansas City, MO  64108

Dear Mr. Hamm:

On behalf of PCI’s nearly one thousand members, we are pleased to submit these initial comments on the NAIC’s draft Principles for Effective Cybersecurity Insurance Regulatory Guidance and Blanks cybersecurity insurance coverage supplement. While cybersecurity is certainly receiving a great deal of scrutiny as of late, it’s important to remember that both regulators and property and casualty insurers have been effectively managing their own cyber risk for quite a long time. What is needed now is not increased oversight of insurers’ own cybersecurity but rather measures designed to facilitate the ability of insurers to satisfy a rapidly increasing demand for cybersecurity insurance. With that said, we offer the following specific comments on the two proposals.

Principles for Effective Cybersecurity Insurance Regulatory Guidance

While many of the concepts and ideas encapsulated by the principles are relatively benign, we are concerned with the publication of new principles, other than those already effectively practiced by regulators and insurers, in that such publication suggests that cybersecurity is either new or that the property and casualty insurance industry is not properly managing their cybersecurity. Property and casualty insurers have long been subject to rigorous state and federal privacy and information protection laws, and the track record of both regulators and the industry is excellent in this regard. Rather than adopt a list of principles, a much better approach is to issue a general policy statement to the effect that any new regulatory requirements with regards to insurers’ cybersecurity should be based only upon an objective finding of gaps and should recommend the least burdensome method of compliance.

With respect to specific principles, we offer the following observations:

- Principle 8 – as previously mentioned, insurers are already subject to regulatory oversight and required to file detailed reports with regards to enterprise risk and solvency. We are concerned that this principle seeks to impose yet another reporting requirement on insurers with respect to cybersecurity. Every effort should be made to limit duplicative requirements on insurers.
- Principle 11 - who exactly is sharing information with whom? Insurers with government agencies? Insurers with other insurers? Both? Additional clarity regarding this principle is needed.
• Principle 14 – there are numerous public and private sector entities that are focused on cybersecurity. Why identify a specific group to join rather than encourage insurers to investigate and consider joining any one of the many such type of groups? We also wonder, again, with whom are insurers to share what kind of information? Additional clarity is required here.

• Principle 15 – we suggest that this principle focus on the protection of data generally, rather than mandating the use of any one particular means of doing so. To the extent the term “encryption” is used, it’s not clear what is meant by the term given that there are currently many standards of encryption currently available.

Blanks

We support adoption of the NAIC cybersecurity insurance coverage supplement form. The collection of information that the NAIC already collects with regards to other lines of insurance should also be collected with regards to cybersecurity insurance and will help inform public policy discussions.

Supporting the Growth of a Cyber Insurance Market

The greatest contribution the NAIC and state regulators could make is to work with the industry to identify where hurdles may exist to the offering of cybersecurity insurance. In addition, it would be beneficial if regulators could work in tandem with the industry to respond to federal inquiries and also help foster the conditions where cybersecurity insurance can grow, consistent with sound financial management.

Based on the property and casualty insurer record in this area, there simply is no need for additional, intrusive regulation. Rather, we respectfully submit to you that a simple policy statement is better than any lengthy set of principles, many of which may very well cause needless complications. A much better approach to cybersecurity insurance is for the NAIC to work together with industry to help facilitate the continued development of the cybersecurity insurance market.

Sincerely,

Thomas M. Glassic
Vice President, Policy and Government Affairs
thomas.glassic@pciaa.net

Alex Hageli
Director, Personal Lines Policy
alex.hageli@pciaa.net

David Snyder
Vice President, International Policy
david.snyder@pciaa.net

Cc: Aaron Brandenburg
    Eric Nordman