ACE

We have concerns with the proposed Supplement. While we appreciate the NAIC's desire to understand the cyber security market, the Supplement does not sufficiently account for the variety of ways in which cyber coverage is issued. For example, the Supplement breaks cyber security coverage into two main categories: "Standalone" and as a component of a Commercial Multi Peril Package. This approach, however, ignores other products in which cyber coverage might be available, as well as the types of cyber risks covered by each. As a result, carriers may have difficulty providing the type of consistent, accurate data that would give regulators a truer picture of the marketplace.

Travelers

There should be something in the supplement that differentiates First party vs. Third party limits for Cybersecurity

PCI

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.

NAMIC

Few concerns identified by NAMIC members with respect to the proposed annual statement supplement the level of detail called for in the supplement may be excessive and could undermine the competitive position of an insurer writing cyber insurance. There was also a suggestion that the supplement should include a means to provide information about reinsurance since that could significantly impact a company’s actual exposure to risk from cyber threats.

AIA

Fundamentally, one of the main concerns with the Proposal is that it does not account for the unique nature of what a cybersecurity policy is. Cybersecurity is a broad term that can encompass many different insurance products. While the Proposal provides a definition for cybersecurity, what is “cybersecurity insurance” for the purposes of this Proposal? Is the intent of this Proposal to elicit information on cyber-like coverages that might be covered under a traditional policy (i.e. cyber extortion under a Kidnap and Ransom policy)? Further, insurers will differ on what is a cybersecurity insurance” product. For example, ISO has described cybersecurity as “E-Commerce” or “Data Privacy and Security.”

(1) What is meant by losses (response reimbursement, business interruption, digital assets, liability coverages, etc.) Does the Proposal want first and third party losses?
(2) What is meant by “Direct Defense” and “Cost Containment?”
(3) How are we to identify “Policies in Force” when the policy could be a hybrid of claims made and occurrence based?
(4) There is no useful way of stating the range of limits. There could be a blend of first and third party coverages, so there could be a policy aggregate and sub-limits. Further, is this limited to a primary policy when the carrier is the sole insurer? If so, this could create additional confusion in the range of limits.
(5) Multi-peril coverage with cybersecurity may not be handled the same way. For example, premium associated with cyber may be able to be estimated in some situations and not in others.
(6) What is meant by “Tail Coverage?” A range of limits may not be possible in this situation.
(7) What is meant by “Paid + Change in Case Reserves?”

Finally, we want to emphasize that the information collected in this supplement is more detailed than what is typically reported in the yellow book for products, particularly counts and limits at the policy level. This is a highly competitive and emerging market and as such the type of data requested and the confidentiality protections in place should be given serious consideration.
The proposed supplement is a basic summary of cybersecurity policies and coverage offered by an insurer. It would be useful as basic information for regulators and the public to see who is actually writing cyberinsurance policies and coverages. However, it is unclear how the proposed supplement would be used by either financial or market regulators for more than simply identifying insurers who offer and sell the coverage. The supplement would not enable regulators to differentiate claims experience relative to premiums (loss ratios), differentiate claims experience for claims made vs. occurrence policies, differentiate policies with minimal exposure vs. substantial exposure for the insurer or identify the frequency of coverage limits employed. For example, the range of coverage limits might be $5,000 to $5,000,000, but without knowing the number of policies or coverages with $5,000 or $5,000,000 limits or amounts in between, the information has little value to financial regulators attempting to assess an insurer's exposure.

We suggest that the public supplement be accompanied by a non-public list of all policies which provide cybersecurity coverage. Each record would be a policy with the following fields:
1. Policy Identifier
2. Standalone or CMP coverage
3. Single State or Multiple State Coverage
4. Effective Date
5. Term of Coverage
6. Policy Form Identifier
7. Claims Made or Occurrence Coverage
8. Direct Premiums Written (If CMP policy, estimate premium portion for cybersecurity coverage)
9. Direct Premiums Earned (If CMP policy, estimate premium portion for cybersecurity coverage)
10. Direct Losses Paid (If CMP policy, report only for cybersecurity coverage)
11. Direct Losses Incurred (If CMP policy, report only for cybersecurity coverage)
12. Loss Case Reserve Beginning of Period (If CMP policy, report only for cybersecurity coverage)
13. Loss Case Reserve End of Period (If CMP policy, report only for cybersecurity coverage)
14. DDCC Paid (If CMP policy, report only for cybersecurity coverage)
15. DDCC Case Reserve Beginning of Period (If CMP policy, report only for cybersecurity coverage)
16. DDCC Case Reserve End of Period (If CMP policy, report only for cybersecurity coverage)
17. Date Claim Received by Insurer
18. Date Claim Denied by Insurer, if denied
19. Date Claim Paid by Insurer, if paid
20. Claim Subject to Litigation (y/n)

The policy-level data would provide essential information to both financial and market regulators. For financial regulators, the detailed information would allow assessment of cyberthreat exposure to the insurer. For market regulators, the detailed information would allow assessment of the frequency and severity of claims and, consequently, the general reasonableness of rates. The loss ratio information would inform market regulators regarding policyholder understanding of policy forms and related claims settlement practices. In total, the data would provide regulators with the necessary information to monitor cyberinsurance markets and practices.

Louisiana

Section 2.2 – Change the first title to read – C

<table>
<thead>
<tr>
<th>Section 2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the first title to read:</td>
</tr>
<tr>
<td><strong>Direct Cybersecurity Coverage Losses</strong></td>
</tr>
<tr>
<td>Change the second title to read:</td>
</tr>
<tr>
<td><strong>Direct Cybersecurity Coverage Defense and Cost Containment</strong></td>
</tr>
</tbody>
</table>
Change 2.4 to read:
If the answer to 2.3 is yes, provide the quantified or estimated direct premium written and earned for cybersecurity coverage in package policies

Add lines to capture Direct Written Premium and Earned Premium for both lines 2.41 and 2.42