555 12th Street NW
Suite 550
Washington, DC 20004
202-828-7100
Fax 202-293-1219
www.aiadc.org

May 24, 2016

VIA EMAIL: cyber.security.insurance@hq.dhs.gov

Matthew Shabat, Director
Director, Performance Management
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

RE: National Protection and Programs Directorate's Cyber Incident Data Repository White Papers

Dear Mr. Shabat:

The American Insurance Association (AIA) welcomes the opportunity to provide feedback regarding the National Protection and Programs Directorate's (NPPD) white papers summarizing the work of the Cyber Incident Data and Analysis Working Group (CIDAWG) to explore the benefits of an anonymized voluntary cyber incident data sharing repository (repository). AIA represents approximately 325 major U.S. insurance companies that provide all lines of property-casualty insurance to U.S. consumers and businesses, writing nearly $127 billion annually in premiums. Many of our members write "cyber insurance" and have a keen interest in the CIDAWG's work both from a product perspective and the broader implications for enhanced cyber resilience. Overall, we appreciate the NPPD and CDAWG's efforts and support the process that the NPPD has undertaken to promote a robust cybersecurity insurance market and cyber resilient country.

Benefits of NPPD's Effort to Explore a Data Repository

Cybersecurity insurance is a valuable risk transfer mechanism. It can also serve as a useful tool to help companies evaluate their own individual cyber risk management posture. To that end, there is a competitive cybersecurity insurance market that continues to grow as insurers innovate and explore new ways to meet increasing market demands. That said, the cyber insurance market is relatively young and one of the challenges to continued market growth and expansion is a lack of robust actuarial data. We appreciate the NPPD effort to promote a robust cybersecurity insurance market through detailed and thoughtful conversations about what a repository would look like. The thought and analysis that has gone into the white papers and bringing Chief Information Security Officers and the insurance industry together alone has been a beneficial step toward understanding ways to shorten the actuarial data gap.

Further, we appreciate that the repository is intended to benefit the broader information security community by creating a benchmarking tool. This enhances our shared devotion to cyber resiliency.

Challenges to an Effective Repository

While we support the concept of an anonymized and trusted data repository, we recognize that significant challenges exist for such a repository to be effective. One key challenge we have observed is ensuring accurate reporting. Certain data categories proposed for the data repository could be susceptible to subjectivity and, as a result, inconsistent reporting among entities. Inaccurate or inconsistent data would, of course, significantly reduce the value of the repository.

Another important challenge is ensuring anonymity and privacy. Anonymity of reporting would be a critical element of an effective cyber incident data repository. However, certain proposed data categories could capture a significant amount of detail, which might compromise the anonymity of the reported incident. An effective cyber incident data repository would need to strike an appropriate balance between level of detail and anonymity.

The security of the repository data is another challenge that cannot be underestimated and it would be worthwhile to discuss what common security standards may be required and how a contributor would meet and agree to these standards.

We recognize that the repository will not be government operated, but the question still remains how, if at all, the government might have access to the data and if the government does have access, what limitations will be placed on its use. This is an important challenge to consider, because the government should also be a contributor to the repository. Therefore, the white papers ought to discuss how the government will share and how they will have access to and/or use the data.

Fundamentally, the challenges highlighted above and in the obstacles white paper (to include the importance of liability protections) culminate into a threshold issue of determining how to maintain the essential voluntary nature of the repository while incentivizing a large number of participants. It has been correctly noted that addressing these obstacles will be complicated and difficult. Some examples of solutions include implementing statutory protections, tweaking data categories, or even expanding the education campaign to ensure that the broader information security community understands that there are benefits beyond cybersecurity insurance. It might also be useful as the challenges discussion continues to link the obstacles white paper and values proposition.

Specific Data Category Suggestions

As the NPPD continues to reflect on this project, we also have the following thoughts as to the data categories:

- In data category #3, a question about whether or not the organization conducts testing may be helpful.
- A DDOS attack seems to be missing from data category #6.
- The second chart in data category #9 overlaps with data category #5.
- The first chart in data category #10 is missing notification by investigative reporter or press.
- “Rerouting traffic” is missing from the tactics, techniques and procedures used to respond to an incident in data category #11.
- Costs identified in data category #14 may consider including “insurance offset, if any.”

Logistical Clarity

Finally, informal conversations and panel discussions with persons not involved in the CIDAWG meetings suggest that there may be a general misunderstanding of the logistics and intended goal of the project. It has been AIA's assumption that companies experiencing a breach would contribute data into the repository on a voluntary basis, a type of after action report. Therefore, insurers are not necessarily entering data unless they are the victim of a hack and have chosen to enter their own incident data into the repository. There seems to be some confusion and a suggestion that insurers would be inputting their customer's data, which would present its own set of challenges and concerns.

Additionally, we are aware that there are questions as to the difference between a cyber-incident data repository, sharing with an Information Sharing and Analysis Organization (ISAO), sharing with an Information Sharing and Analysis Center (ISAC), and real-time threat sharing as permitted by the Cybersecurity Information Sharing Act (CISA). The many portals for sharing cyber information can be somewhat daunting and time consuming. It might be a worthwhile to clarify the differences between the NPPD contemplated incident repository and the other information sharing platforms. Further, it might be valuable to start a dialogue to think through how, in the future, information sharing of threats and incident data through portals could be integrated.

Again, we appreciate the NPPD and CIDAWG effort to promote a robust cybersecurity insurance market and a more resilient country. We also agree with the potential benefits of an anonymized and trusted data repository. In general, sharing of cyber threat intelligence and cyber incident information will increase resilience to cyber risk. Additionally, sharing of cyber incident and loss information will support the growth of the cyber risk insurance market. However, the obstacles document and comments above evidence that there are many questions that still need to be answered and we look forward to continuing to work with you on this project. In the end, the conversations and white papers have already added value to ongoing data discussions.

Respectfully submitted,

Angela Gleason
Counsel