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

Americas Regulatory Risk Management
101 Constitution Avenue, NW Suite 700
Washington, DC 20001
Phone +1 (202) 742 4635
Matt_McKenney@swissre.com

May 24, 2016

Swiss Re Comments on Cyber Incident Data Repository White Papers
Delivered Electronically

Dear Mr. Shabat:

Swiss Re respectfully submits this comment letter in response to the request for comments on the National Protection and Programs Directorate Cyber Incident Data Repository White Papers. Swiss Re is a 152-year-old global reinsurance company that has helped America recover from disasters since the San Francisco earthquake of 1906. Swiss Re has several thousand highly-skilled employees in more than thirty offices throughout the United States. Swiss Re was the first reinsurer to create a unit dedicated to working with governments to deploy risk transfer solutions and reduce the exposure of the taxpayer to insurable risks.

Introduction
Swiss Re appreciates the Department of Homeland Security's (DHS) effort to promote a robust cybersecurity insurance market, in order to improve public and private sector resilience to cyber risk. We agree with DHS's view on the potential benefits of an anonymized and trusted data repository. Swiss Re believes the sharing of cyber threat intelligence and cyber incident information between the public and private sectors will increase resilience to cyber risk and will support the growth of the cyber risk insurance market. Importantly, information sharing must be conducted in a manner that is consistent with legal and contractual obligations, and that protects the privacy of sensitive personal information.

Challenges to an effective data repository
While we support the concept of an anonymized and trusted data repository, we recognize significant challenges exist for such a repository to be effective. One key challenge is ensuring accurate reporting. Certain data categories proposed for the data repository could be susceptible

to subjectivity and, as a result, produce inconsistent reporting among entities. Inaccurate or inconsistent data would significantly reduce the value of the repository.

Another important challenge is ensuring anonymity. Anonymity of reporting is a critical element of an effective cyber incident data repository. However, certain proposed data categories could capture a substantial 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.

Importance of a common codification
Data sharing is only meaningful and effective if the data can be aggregated and analyzed. This must be enabled by common codification and taxonomy for cyber incidents and losses and would facilitate greater understanding of cyber threats, which can improve society's cyber resilience. Additionally, the common codification standards and taxonomy facilitates the underwriting and pricing of cyber risk.

To this end, Swiss Re is working with the CRO Forum to propose a categorization methodology for cyber risk. The objective is to capture cyber incident data using a common language, so that the data can be aggregated and analyzed. The proposed methodology relies on existing cyber incident reporting that occurs within IT and Risk Management functions, in order to encourage consistent data capture and reporting. A CRO Forum concept paper on its proposed categorization methodology for cyber risk is forthcoming.

Conclusion
Swiss Re appreciates the opportunity to provide our views on this important topic. We look forward to a continued dialogue with DHS and other stakeholders on our shared objective of improving cyber resilience, including through effective cyber incident data sharing.

Kind regards,

Swiss Re Americas