U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

May 24, 2016

Via cyber.security.insurance@hq.dhs.gov

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

Subject: National Protection and Programs Directorate; National Protection and Programs Directorate Seeks Comments on Cyber Incident Data Repository White Papers[1]

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, appreciates the opportunity to comment on the creation of a cyber incident data and analysis repository (CIDAR or repository). The "cyber" insurance market is on the rise, and the Chamber wants to help it grow soundly beyond a few key sectors (e.g., banking and financial services, health care, retail, and technology) and large organizations, which are the principal buyers of coverage today.[2]

The Chamber does not attempt to answer every question in the Department of Homeland Security's (DHS') notice requesting public feedback. Instead, the Chamber (1) stresses the need for data anonymization, (2) recognizes the possible need for additional sharing protections, and (3) believes that a CIDAR pilot program can offer tangible upsides to public- and private-sector cybersecurity. More comprehensive information could assist insurers in developing both cyber coverage and risk management solutions and best practices for their customers.

First, the Chamber believes that the organizations submitting cyber incident data must be made anonymous. Most organizations do not want to be publicly revealed, much less acknowledged within the sharing ecosystem, as contributors to the CIDAR. DHS has taken note of this issue.

---

[1] https://federalregister.gov/a/2016-06856

[2] www.commerce.senate.gov/public/index.cfm/2015/3/examining-the-evolving-cyber-insurance-marketplace, https://homeland.house.gov/hearing/the-role-of-cyber-insurance-in-risk-management

Second, many organizations understand that exchanging cyber incident data and contributing to a CIDAR could generate significant value for multiple parties. But it is not clear to the Chamber that organizations would contribute information at sufficient scale to make a CIDAR function successfully without addressing real or perceived concerns related to liability, regulatory, public disclosure, and antitrust matters.

Existing laws and policies may offer organizations the protections that they believe are necessary to engage in bidirectional sharing. However, supporters of a CIDAR should recognize that legislation may be necessary to safeguard organizations that want to voluntarily share and receive cyber incident data vis-a-vis a repository. The Chamber is not arguing for legislation yet. But our experience with advocating for cybersecurity information-sharing legislation suggests that organizations' fear of liability can be a central barrier to the constructive exchange of cyber incident data (e.g., the type and severity of an incident, costs, and contributing causes).

Third, the Chamber believes that an experimental CIDAR is worth pursuing. DHS officials have suggested that a repository would have to begin with what actual information currently exists and then build from there to provide the full context when a cyber incident occurs of what happened and what was the response. According to DHS' summary of its April 2016 cyber repository workshop, "A CIDAR pilot should start with basic, useful, and easy-to-acquire data categories in order to gain market acceptance. Over the longer term, data input must be practical—and if possible automated. Companies that experience thousands of 'incidents' a week are not going to hire 15 extra people just to do voluntary data reporting."

DHS also acknowledges that in many cases the specifics of a cyberattack are not immediately known and that a pilot repository would have to be flexible enough to allow updates.[3] Such thinking seems logical to the Chamber, and it tracks with our experience.

***

The Chamber welcomes the chance to provide feedback on the creation of a CIDAR. Given recent high-profile cyber incidents, cyber insurance is fast becoming a need for commercial customers. However, as a new market, insurers face a number of challenges, such as aggregating sufficient data to better comprehend what best practices are ideal in a given sector and to offer and price insurance products competitively, including to critical infrastructure.

Cyber insurance is not a substitute for strong information network and system defense. Still, a robust cyber insurance market can be an important tool to help organizations utilize sound standards, guidance, and best practices—especially ones highlighted in the joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*—in return for more coverage and lower premiums.

[3] "DHS details steps for piloting cyber-data repository for insurers," *Inside Cybersecurity* (May 19, 2016). http://insidecybersecurity.com/daily-news/dhs-details-steps-piloting-cyber-data-repository-insurers

If you have any questions or need more information, please do not hesitate to contact me (abeauchsene@uschamber.com; 202-463-3100) or my colleague Matthew Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne