The Global Voice of the Tech Sector

U.S. CHAMBER OF COMMERCE

July 25, 2017

Thomas McDermott
Deputy Assistant Secretary for Cyber Policy
Office of Cyber, Infrastructure,
and Resilience Policy
Department of Homeland Security
Washington, DC 20016

Adam Sedgewick
Technology Policy Advisor
Office of Policy and Strategic Planning
Department of Commerce
Washington, DC 20230

Brian Peretti
Director, Office of Critical Infrastructure Protection
and Compliance Policy
Department of the Treasury
Washington, DC 20220

Dear Messrs. McDermott, Sedgewick, and Peretti:

The Information Technology Industry Council (ITI) and the U.S. Chamber of Commerce write to express appreciation for meeting with us on July 13 to discuss the provision of the administration's cybersecurity executive order (EO) regarding Supporting Transparency in the Marketplace. We strongly believe that existing federal policies and practices sufficiently promote the market transparency of publicly traded critical infrastructure companies' cyber risk management practices.

Our groups, for example, recognize the importance of SEC Chairman Jay Clayton's recent statement, "Public companies have a clear obligation to disclose material information about cyber risks and cyber events." Indeed, companies take their requirement to disclose material information about cyber risks and events in a timely and accurate manner seriously. Critical infrastructure entities, which are a focus of the EO, work diligently to manage cyber risks holistically against a range of threats. Corporate leaders increasingly view their enterprises' information security as a leadership issue and market differentiator. Robust cybersecurity contributes to a company's bottom line and resilience.

Since the EO's release in May, we are encouraged that department officials seem disinclined to propose additional disclosure requirements on the business community. This reluctance makes sense given that registrants' decisions whether to disclose cybersecurity risks turn on individualized analyses of the materiality of such risks. However, we especially want to highlight our thinking for your agencies' forthcoming report to the White House.

Looking ahead, government agencies should strengthen their cooperation with businesses to beat back cyberattacks in concerted ways, not blame the victims of cyber incidents. Adding more red tape could easily disrupt or damage trusted relationships between industry and government needed to counter malicious hacking. Companies do not want to see valuable public-private partnerships harmed because of new reporting rules. Going beyond current disclosure policies and practices could compromise registrants' cybersecurity and paint a target on their backs—including industry peers and supply chain partners—with no appreciable benefit accruing to investors.

In addition, the Department of the Treasury's June report calling for streamlined cyber regulatory requirements is a constructive step. It urges better coordination among financial agencies to enhance the resilience of the sector. Treasury's report is relevant because several federal bodies mandate companies disclose their cyber risks and management practices. Rather than expanding critical infrastructure entities' disclosure workload, the administration should give thought to reducing regulatory fragmentation and overlap among sectors.

Our associations contend that current federal policies and methods amply promote the transparency of publicly traded critical infrastructure companies' cyber risk management practices in the marketplace. We look forward to continuing our work together to advance the security and resilience of the business community and the nation.

Sincerely,

Information Technology Industry Council (ITI)
U.S. Chamber of Commerce