CYBER
U.S. CHAMBER OF COMMERCE

CYBER, INTELLIGENCE, AND
SUPPLY CHAIN SECURITY DIVISION

Initiatives Summary

Cybersecurity
LEADERSHIP COUNCIL

The Cybersecurity Leadership Council functions as Cyber, Intelligence, and Supply Chain Security Division's (CISD) advisory board and sets the Chamber's cyber policy priorities. Both the Cyber Working Group and the National Security Task Force (discussed below) are influenced by the guidance and recommendations of the council. The council is made up of approximately 30 members representing mostly large and midsize businesses across multiple sectors, along with associations and universities. Council members inform policy decisions and engagement with the executive and legislative branches and guide Chamber policy positions on emerging issues, such as 5G, IoT, and cyber deterrence.

- Council members meet monthly with senior government officials in an intimate setting to foster discussion and relationship building. Meetings are off the record. By way of example, we have hosted meetings with the executive director of the U.S. Cyberspace Solarium Commission and his senior staff (three times since September 2019); members of Congress (e.g., Jim Langevin, Roger Wicker) and professional committee staff; DHS Cybersecurity and Infrastructure Agency leadership, including Director Christopher Krebs, Jeannette Manfra, Bob Kolasky, and Brian Harrell; Department of Energy Assistant Secretary Karen Evans; Federal CISO and NSC Senior Director for Cybersecurity Policy Grant Schneider, among others.
- Cyber Leadership Council members have exclusive access to senior civilian, intelligence, defense, and law enforcement officials, which enables them to advance their public policy objectives and mature these relationships.

Cybersecurity
WORKING GROUP (CWG)

The CWG conducts the day-to-day policy work on priorities set by the Cybersecurity Leadership Council. This group is made up of approximately 200 companies, associations, and state and local chambers. Through a weekly call and regular email communications, we identify current legislative and regulatory issues that could positively—or negatively—affect the business community. Through this persistent engagement, we craft approaches to advance, shape, or block such issues, as appropriate.

- An example of work done by the CWG, in conjunction with guidance from the Cyber Leadership Council, is a funding request drafted by the Chamber and submitted to the Senate Appropriations Committee for a $5 million pilot program to embed analysts from the U.S. Intelligence Community (IC) with private sector critical infrastructure entities. The goal of this voluntary program is to make private sector entities customers of the IC for purposes of collective cyber defense and demonstrate the value of such a partnership for both government and the private sector.

National Security **TASK FORCE**

The National Security Task Force (NSTF) encompasses more than 400 companies, associations, and state and local chambers. As such, its policy focus is broader than the Cyber Leadership Council or the CWG. The NSTF serves largely as a policy deployment and education mechanism through outreach to Congress, regulatory filings with agencies, engagement with executive branch departments and agencies, and communications with the media, elected and appointed officials, and members of the business community.

The NSTF makes recommendations and offers solutions to Washington leaders on an array of homeland and national security challenges, including cybersecurity issues, critical infrastructure protection and resilience, global supply chain matters (both physical and IT related), and customs and trade facilitation. The NSTF meets twice annually.

Project **SECURITY**

Project Security is a joint initiative between the Chamber's Center for Global Regulatory Cooperation and the Cyber, Intelligence, and Supply Chain Security Policy Division. The project promotes international cybersecurity norms and resilience, encourages innovation, and advances a reduction of the global regulatory and compliance burdens for cybersecurity practitioners.

Project Security represents every segment of the economy, from energy and electric companies to manufacturing, retail, and financial services. It engages regularly and directly with foreign governments on cyber policy issues and represent the interests of the American business community abroad where appropriate.

Cyber **SERIES**

Each year the Chamber hosts a series of single-day events in target cities around the country to promote cyber education and build relationships between the private sector and government cybersecurity and law enforcement agencies. In 2019, we held events in Hartford, Connecticut; Houston, Texas; Seattle, Washington; and San Diego, California.

The target audience for these events is midsize and small businesses. Presenters include cybersecurity experts from among our member companies, senior government and elected officials, and law enforcement leaders. This series culminates annually with the Chamber's Cyber Week in Washington, D.C. Four policy programs over four days bring together roughly 1,000 public and private stakeholders and offer presenters an opportunity to reach broad audiences—potentially untapped ones.

- 2019 cyber series events featured a select number of Chamber members as panelists and keynote speakers, including AT&T, Deloitte, FICO, Qualcomm, RSM, and T-Mobile.
- These events showcase Chamber member company expertise and draw in senior government leaders, such as Bill Evanina (ODNI/NCSC), Amy Hess (the FBI), Christopher Krebs (CISA), and others from U.S. Cyber Command and other government agencies.
- Underwriters of the Chamber's Cyber Series have access to attendee data, enabling them to pursue marketing and business development opportunities that extend well beyond discussions at the events.