January 2018

NATIONAL AND CYBER SECURITY

What We Believe: Economic security and national security go hand-in-hand. We must have one in order to protect the other. The Chamber advocates for protecting vital U.S. assets—both physical and digital—to ensure the safety and security of our citizens and promote the free flow of commerce and information that drives our economy and enriches our society.

> Even as we work to advance technology in our economy, we must also safeguard businesses and consumers from its risks, including cyber attacks and data privacy breaches.

Priorities for 2018

- Make practical updates to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (version 1.1), while ensuring that the standards remain voluntary and enjoy broad support from the business community.
- Clarify federal and industry roles and responsibilities in protecting from, responding to, investigating, and prosecuting cybercrime. Ensure that the departments and agencies tasked with these responsibilities have the resources and the interagency coordination they need to excel.
- Work with Congress and the Department of Homeland Security to expand the SAFETY Act, which provides liability protections for qualified anti-terrorism technologies, to cover products and services used to prevent or counter significant cyber incidents.
- Advocate that the final text of the European Commission's expected Cybersecurity Strategy update, which will call for minimum cybersecurity standards, certification requirements, and trust labels for all IoT devices, include:
  - Use of the NIST Framework,
  - Mechanisms to grow the cyber threat information sharing ecosystem,
  - And promotion of principles for IoT security.

U.S. CHAMBER OF COMMERCE