CYBER
U.S. CHAMBER OF COMMERCE

CYBER, INTELLIGENCE, AND
SUPPLY CHAIN SECURITY DIVISION

Policy Priorities

The Chamber urges domestic and international policymakers to champion the following proposals. We believe that they are risk based, effective and actionable, and aligned with many public sectors objectives.

FOSTER U.S. CYBER AND ECONOMIC RESILIENCE

- Government and industry should actively promote the National Institute of Standards and Technology's Cybersecurity Framework (the Framework) in the U.S. and internationally.
- The U.S. Congress should pass legislation that grants users of the Framework legal liability protections to strengthen business resilience and certainty. Positive incentives would broaden the use of the Framework and quicken national response and recovery efforts in the wake of a significant cyber incident.
- Increased use of the Framework by the business community should be paired with an energized federal effort to streamline cyber regulations.

INCREASE THE DEFENSE OF THE INTERNET ECOSYSTEM

- The U.S. Congress should pass federal Internet of Things (IoT) cyber legislation that reflects the consensus IoT security baseline, protects device makers and buyers from liability, and reduces policy fragmentation globally. The bill should preempt state laws and regulations. Federal legislation would bolster U.S. security and demonstrate leadership at home and abroad.
- The U.S. Congress should modernize the SAFETY Act through a legislative fix. Increasing the number of SAFETY Act-approved cyber technologies that are deployed throughout companies and agencies would reduce cyber risks that the public faces from rampant state-backed and criminal hacking.

PROMOTE INTERNATIONAL NORMS AND DETERRENCE IN CYBERSPACE

- For the past few years, non-governmental groups and companies have taken the initiative to push for norms of responsible state behavior. However, the administration should remain engaged globally to persuade countries to join the U.S. side, including partnering with industry on cyber norms development and promotion.
- A public-private dialogue on challenging topics like sanctions is needed to improve cyber conflict management. Sanctions should be linked to specific foreign policy aims, be multilateral and conduct based, and avoid overreach, among other considerations.
- The U.S. policy shift concerning persistent engagement with our adversaries should be examined by policymakers. Little is known how the change in doctrine would play out in practice. To be successful, persistent engagement should factor in both U.S. government and industry goals.

IMPROVE PUBLIC-PRIVATE COLLABORATION AND SITUATIONAL AWARENESS

- The U.S. Congress should establish and fund a critical infrastructure and intelligence community cybersecurity risk mitigation program (the cyber program) at the Office of the Director of National Intelligence. The cyber program would facilitate the voluntary designation of critical infrastructure entities as customers of the U.S. intelligence community (IC).
- The cyber program would represent a key step toward deeper, more structured bilateral relationships, including activities related to defend forward and persistent engagement, than the current cyber information-sharing process.
- Policymakers should make cyber threats against critical infrastructure a priority across the IC and foster relationships between the private sector and all members of the IC, as appropriate. Currently, a program for routine public-private analytic efforts does not exist.

ENABLE DEFEND FORWARD ACTIVITY TO SUPPORT U.S. CRITICAL INFRASTRUCTURE

- The cornerstone of U.S. cyber strategy should be defense and resilience. But there is a consensus that defense alone is insufficient to disrupt or deter pernicious cyber operations, particularly those launched by states or their surrogates and other malicious actors.
- The administration's 2018 Cyber Strategy offers a potentially sensible approach to U.S. cybersecurity, specifically the principle of defend forward, which emphasizes disrupting or defeating malicious cyber operations at their source.
- The U.S. Congress should legislate the concepts underpinning defend forward as key elements of America's cybersecurity architecture. Legislation should also state that DoD and U.S. Cyber Command (USCYBERCOM) are both authorized and urged to help defend the private sector. The Chamber urges DoD/USCYBERCOM to show restraint in the area of cyber offense.
- Policymakers should ensure that all instruments of U.S. power are engaged at the earliest moment against significant cyber threats to protect American interests and promote stability and responsible state behavior in cyberspace.

OPTIMIZE GOVERNMENT STRUCTURES AND FUNDING

- Policymakers should continue to clarify the rights, roles, and responsibilities of the public and private sectors, including backing a proposed model of Defense Support to the Private Sector.
- Government should proceed cautiously concerning recommendations that establish new federal bodies, particularly ones that would have regulatory authority. Existing agencies should be pressed to excel and be held accountable. Any new organization should fill a demand that is not already being met—or that could be met—by an existing institution.
- The Chamber recommends that cybersecurity management roles at the White House (e.g., cyber coordinator) and the U.S. Department of State (e.g., cyber ambassador) need to be elevated to strengthen intragovernmental coordination and engagement with the private sector.
- The U.S. administration and the U.S. Congress should collaborate with the private sector to take a more active and risk-based approach to U.S. engagement in international cyber standards bodies. The White House should request, and Congress should appropriate, additional funding for the U.S. Department of Commerce to facilitate international cyber standards efforts side by side with the business community.
- The executive branch should support investing in and expanding the U.S. network of Mutual Legal Assistance Treaties (MLATs). It should urge the U.S. Department of Justice (DOJ) to create a private-sector advisory board to write and implement international agreements called for under the Clarifying Lawful Overseas Use of Data (CLOUD) Act.

U.S. CHAMBER OF COMMERCE
CYBER, INTELLIGENCE, AND SUPPLY CHAIN SECURITY DIVISION