U.S. Chamber of Commerce

U.S. Chamber of Commerce
Cybersecurity Policy Principles

The federal government's role in addressing cybersecurity is complex and expansive. Its engagement includes mitigating risks and threats to agency systems and working with the private sector to better protect business networks and assets from malicious actors.

During the past few years, Congress has enacted several bills that address various aspects of cybersecurity, such as information and network security, device security, organizational governance, and supply chain security. In addition, recent administrations have promulgated numerous policies that range from relatively simple guidance to sweeping, prescriptive regulation.

The U.S. Chamber believes that the government's involvement in cybersecurity is laudable and increasingly necessary for many reasons, as evidenced by the foreign cyber intrusion campaign against SolarWinds and public- and private-sector entities. When constructed and implemented well, public policy can promote national and economic security, resilience, transparency, accountability, and trust among many public and private organizations. Indeed, optimal approaches to cyber risk management draw on proactive, steady, and informed collaboration between government and industry.

This document is basically a cheat sheet that highlights the U.S. Chamber's thinking on some key cybersecurity themes and issues.[i] We urge the 117th Congress and the Biden administration to consider them as they develop new policies, laws, and regulations and/or revise existing ones.

The paper's topics are summed up in seven words—potential, program, protection, preemption, partnership, price, and promotion. Further, the paper covers how the U.S. Chamber will assess legislation, advocate for balancing federal regulation with industry protection, consider the costs of cybersecurity, seek mutually beneficial agreements with policymakers, and promote U.S. policies at home and internationally.

1. Potential

"Potential" refers to the call for organizations to be more open to unexplored policy opportunities than they've traditionally been. Cybersecurity legislation is often written between the divergent poles of regulation and nonregulation, with final bills sometimes leaving parties dissatisfied with the outcomes. Thus, there is much potential for negotiating parties to seek agreements that are fair and beneficial to all sides.

- Cyber policies and legislation should advance the interests of both policymakers and businesses. Parties should strive to work outside their comfort zones, which the U.S. Chamber will endeavor to do as well.

- To advance positive discussions and mutually beneficial trade-offs, parties should establish that no measures are agreed to until everything is agreed to.

2. Program

The U.S. Chamber is constantly seeking ways to work with lawmakers to strengthen the cybersecurity environment for governments, businesses, and consumers. We are especially interested in advancing innovative cybersecurity policies and laws—a mix of carrots and sticks—that carefully balance regulatory compliance with industry- recognized standards and positive incentives to increase U.S. security and resilience commensurate with today's threat levels.

* This document was prepared by the U.S. Chamber's Cyber Leadership Council and Cybersecurity Working Group, which are led by the Cyber, Intelligence, and Supply Chain Security Division. It's worth noting that Project Security, also a Chamber program, handles the organization's international cybersecurity efforts.

- Congress should generally write legislation to motivate businesses to demonstrate their use of existing standards, guidelines, and frameworks to meet a regulation's and/or a law's requirements. In exchange, businesses would qualify for congressionally crafted protections and other inducements to invest in and meet heightened cybersecurity requirements.

- Where applicable, legislation should offer private parties a menu of appropriate standards, guidelines, and/or frameworks to select from, facilitating choice and the buy-in of regulated parties.[ii] Relatedly, programs should establish reciprocity requirements to harmonize laws, regulations, and other obligations.

- Congressionally created programs should be flexible (e.g., scalable to a business' size and budget) and risk-based, thus targeting industry's resources at legitimate threats and harms. Also, definitions should be clear and reflect market conditions and businesses' practical experiences.

3. Protection

Businesses confront relentless, often state-sponsored, cyberattacks but frequently lack effective government protection. Cyberspace remains the only domain where we ask private companies to defend themselves against nation states and/or their proxies. The U.S. Chamber believes that this security gap justifies blending a mix of new cybersecurity requirements with regulatory and legal protections.[iii]

- The U.S. Chamber urges Congress to incentivize the behavior of industry members, such as manufacturers, developers, and vendors, by granting liability protections. These safeguards would benefit organizations that take additional steps to improve cybersecurity.

- Depending on the nature of the program, liability protections should range from an affirmative defense (sometimes referred to as a safe harbor) against lawsuits to more comprehensive protections against litigation generated by a cyberattack.

- Lawmakers should restrict federal, state, and local agencies from using cybersecurity information that businesses share with the government to directly regulate a private entity's lawful activities.

4. Preemption

As new cybersecurity laws continue to be enacted domestically and internationally, businesses are routinely forced to navigate a crowded patchwork of obligations, which is particularly pronounced in cybersecurity and data protection. Adopting risk-based legislation while establishing clear and consistent federal guidelines would ensure that both regulators and regulated entities can direct scarce resources at significant cybersecurity risks.

- Congress should preempt state laws to provide national uniformity and align duplicative and often conflicting compliance burdens by overriding or deferring to a specified law. Greater business certainty would drive investments in better cybersecurity risk management and adherence to laws and requirements.

5. Partnership

The U.S. Chamber is proud of the policy, operational, and educational partnerships that we have cultivated with Congress, federal agencies, and state and local governments. The U.S. Chamber is consistently a resource to many policymakers and seeks to solve problems that government and industry each faces but are difficult to tackle alone.

- Government officials should make the private sector (e.g., owners and operators of critical infrastructure, security software and services companies) a partner in crafting cybersecurity policies, including ones related to network defense and incident reporting, standards development, and regulation.

- The U.S. Chamber urges Congress and the Biden administration to provide opportunities for private sector engagement on new legislation and cybersecurity programs, including presidential directives that were promulgated during the Trump administration.

6. Price

"Price" generally refers to the costs and tradeoffs associated with defending an organization in cyberspace, including against America's adversaries. Cyberspace is ubiquitous in our lives and generates extraordinary value for the U.S. economy. However, it can also expose businesses, government bodies, and people to digital risks and threats. Today, the costs of malicious cyber activity (e.g., ransomware attacks) are borne by the victims of cyberattacks.

The U.S. Chamber believes that the government has an obligation to protect American interests against threats to our national and economic security. But we realize that cyberattacks cannot be handled exclusively by the government (e.g., law enforcement, the military, and the intelligence community) or industry. The U.S. Chamber urges businesses to invest in cybersecurity—yet defending against foreign powers and criminal groups can be expensive.

- Policymakers can help mitigate industry's cybersecurity costs, for instance, through streamlining and minimizing the duplications of regulations to better channel businesses' resources toward managing risks.[iv]

- To better protect the federal government in cyberspace, policymakers can assist by making technology capabilities, not pricing, the primary factor when officials procure cybersecurity products and services.

7. Promotion

It is important for the U.S. government, such as the departments of Commerce and State, to collaborate with American industry to promote international consensus on cybersecurity governance. Bridging differences between the U.S. and other countries should help ensure that stakeholders' security concerns are adequately addressed and that cyber requirements do not create trade barriers or limit American firms' access to foreign markets. Thus, the U.S. Chamber urges federal officials to pursue the following objectives as they promote U.S. cybersecurity policies abroad:

- *Push for U.S. leadership in international cyber forums.* Standards, guidance, and certification schemes relevant to cybersecurity are typically led by the private sector and adopted on a voluntary basis. As we move to heightened global cybersecurity standards and laws, it is important that the U.S. asserts its views and leadership.

- *Reduce regulatory fragmentation.* A fragmented global cybersecurity environment creates much uncertainty for organizations and splinters the resources that businesses devote to activities ranging from sound product development, production, and assessments to supply chain risk management.

- *Spotlight global alignment with industry-led baselines.* The U.S. Chamber believes that enterprises in the U.S. and overseas should align their cybersecurity laws and policies with the common language of the joint industry-National Institute of Standards and Technology *Cybersecurity Framework* and the core Internet of Things (IoT) security baseline, which are rooted in international standards and cutting-edge business practices.[v]

Summary

The U.S. Chamber will use its cyber policy priorities to evaluate cybersecurity policies, laws, and regulations and looks forward to working with Congress and other policymakers to negotiate creative policy and legislative outcomes that address multiple interests.

Here are some questions that lawmakers could ask as they consider bills:

- Would the bill create a new regulatory program, or would it draw on and/or improve an existing one? Would the bill offer businesses a menu of industry-led standards, guidelines, and frameworks to select from to

satisfy conformance?

- Would the bill preempt state laws where applicable?
- To what extent would the legislation help harmonize federal laws or rules with U.S. states and international ones? Or would the legislation exacerbate policy fragmentation?
- What would the legislation do to impose costs on malicious actors?
- Would the bill help lessen companies' costs of defending themselves and the U.S. against our adversaries and their surrogates?
- Would the legislation authorize legal liability and regulatory protections for private entities that demonstrate conformance with industry-recognized programs, as well as new laws and requirements?

Notes

---

[i] This document draws on existing U.S. Chamber cybersecurity polices that include Internet of Things (IoT), norms and deterrence, supply chain resilience, information sharing and incentives, and encryption.

[ii] The 2018 Ohio Data Protection Act (S.B. 220) is a notable model that the U.S. Chamber supports. Ohio enacted this innovative data security/cyber law in November 2018. S.B. 220 grants an affirmative defense against data breach tort claims to those businesses whose cybersecurity plans leverage an acceptable industry standard; other states' data protection laws focus on requirements or penalties. The Ohio statute uses an affirmative defense to incentivize companies to improve their cyber practices.

[iii] The Cybersecurity Information Sharing Act of 2015 (see title N of P.L. 114-113), which had the support of both parties in Congress and the Obama administration, is a good example of a program that encourages businesses to defend their computer systems and share cyber threat data with government and private entities within a protective policy and legal structure.

[iv] For several years policymakers have wanted to align and deconflict legislation and rules to increase U.S. cybersecurity through improved efficiency. But federal laws and rules have accumulated with little to no coordination among Congress, agencies, and regulated parties.

[v] The *Cybersecurity Framework* and the core IoT security baseline are key programs that offer a common language and practices that are used across multiple sectors. They also illustrate which programs can be leveraged in conjunction with regulatory and legal liability safeguards to increase business and U.S. security and do not require direct outlays of taxpayer monies.

(Last updated on January 4, 2024)