Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

December 17, 2024

Legislating on Cybersecurity

Introduction

Cybersecurity considerations for policymakers are broader than those for managing cybersecurity at an organization. When thinking strategically about how to legislate for cybersecurity, lawmakers may consider educating, recruiting, and retaining knowledgeable workers; authorizing and resourcing agencies; deterring and responding to threats; securing international supply chains; and understanding the resiliency of individual companies and sectors.

This In Focus discusses key cybersecurity threats and impacts, how Congress has addressed cyber risk, and some general actions policymakers may consider in the future.

Threats and Impacts

The nation faces many threats in cyberspace. Threat actors may directly target the elements of cyberspace (e.g., networks and data) or use those elements to attack public and private entities. The 2024 *Annual Threat Assessment of the U.S. Intelligence Community* discusses five main threat actors: the People's Republic of China (China), the Russia Federation (Russia), Iran, North Korea, and criminals. (Quotes below are from the *Assessment*).

China is "the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks." Recently, China compromised telecommunications systems to spy on campaigns, federal officials, and sensitive government operations.

Russia "views cyber disruptions as a foreign policy lever to shape other countries' decisions and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets." In 2021, Russia compromised a technology services company so it could spy on that company's clients.

Iran is "growing expertise and willingness to conduct aggressive cyber operations" and takes an "opportunistic approach" to attacks. In 2022, Iran exploited a severe bug in widely used open-source software to attack web servers.

North Korea poses "a sophisticated and agile espionage, cybercrime, and attack threat" and focuses on attacks which lead to financial gain. North Korea has long used ransomware and hack-and-leak operations to steal money and bolster North Korea's economy.

Criminal groups are likely to continue to be "involved in ransomware operations … extorting funds, disrupting critical services, and exposing sensitive data." Earlier this year, criminals deployed ransomware on systems that forced a company to degrade their services, snarling healthcare delivery nationwide.

Not all cyber incidents are caused by malicious actors. A computer glitch resulted in mass transportation and commerce disruptions in 2024.

Recent Congressional Actions

For more than a decade, Congress has taken a sustained interest in cybersecurity policy.

The 113th Congress (2013-2014) authorized many existing executive branch activities. Congress directed the Department of Homeland Security (DHS) to serve as the interface between the private sector and the government for cybersecurity matters, and gave DHS a role in the management of federal agencies' cybersecurity.

The 114th Congress (2015-2016) expanded agency authorities. Building on the previous Congress's work, this Congress increased agency responsibilities for cyber information sharing, required federal cybersecurity protection actions, and directed strategy development.

The 115th Congress (2017-2018) created the Cybersecurity and Infrastructure Security Agency (borne out of an existing organization within DHS) to manage national cyber risk.

The 116th Congress (2019-2020) sought to improve interagency coordination. It created a Senate-confirmed position in the White House to coordinate federal agency actions and resourcing for cybersecurity.

The 117th Congress (2021-2022) increased cyber security resources. This Congress provided $4 billion in new funding for federal agencies, state and local governments, and the private sector to modernize information technology and improve cyber resilience. It also created a requirement for private entities to report to the government when they experience cyber incidents and make ransomware payments.

The 118th Congress (2023-2024) added and clarified roles for the Department of Defense and Department of State.

Legislative Activity

During each of the past six Congresses, Members have introduced more than 40 pieces of legislation related to cybersecurity. Approximately half of those got committee consideration, and a smaller number were passed (or adopted) by either the House or Senate. A portion of those became law, either as part of a broader package (e.g., the National Defense Authorization Act) or stand-alone

legislation. **Table** 1 shows the number of *cyber* bills that were considered, passed a chamber, or became a law during each of the 113th to 118th Congresses.

Table 1. "Cyber" Legislation
113th to 118th Congresses (2013-2024)

Cong.	Bills	Cons.	Passed a Chamber	Became Law
118	54	26	6	3
117	110	41	30	14
116	75	23	15	4
115	113	46	37	13
114	70	34	29	6
113	43	20	19	8

Source: CRS analysis of pieces bills and joint resolutions that matched the search term "cyber" on congress.gov through December 9, 2024.
Notes: Congress (Cong.) Considered (Cons.).

Nearly every committee in the House and Senate has been referred a bill addressing cybersecurity. House Rule XII allows for legislation to be referred to multiple committees. Measures in the Senate are usually referred to a single committee under Senate Rule XVII. Taking that into account, the congressional committees that received, considered, and reported (or had discharged) the highest number of cyber bills are displayed in **Error! Reference source not found.2**.

Table 2."Cyber" Bill Activity by House and Senate Committee
113th to 118th Congresses (2013-2024)

	Ref.	Cons.	Rep./Dis.
House Committee			
Homeland Security	86	40	28
Foreign Affairs	53	18	11
Judiciary	49	11	8
Oversight and Accountability	47	18	9
Armed Services	45	10	11
Science, Space, and Technology	39	15	10
Energy and Commerce	35	12	11
Education and the Workforce	29	4	1
Intelligence	29	9	10
Financial Services	22	4	3
Transportation and Infrastructure	22	11	10
Ways and Means	22	7	7
Senate Committee			
Homeland Security and Governmental Affairs	70	48	45
Foreign Relations	34	18	11
Commerce, Science, and Transportation	32	17	14
Armed Services	26	7	8
Judiciary	25	9	13
Intelligence	13	13	13
Small Business and Entrepreneurship	13	11	9
Energy and National Resources	11	9	7

Source: CRS analysis of bills and joint resolutions that matched the search term "cyber" on congress.gov.
Notes: Includes House Committees with over 20 referred bills, and Senate Committees with over 10 referred bills. Referred (Ref.). Considered (Cons.). Reported (Rep.). Discharged (Dis.).

Policy Options

Congress has many options available if it chooses to consider actions related to cybersecurity.

With regard to federal agencies, Congress can assess and allocate resources, establish programs, and conduct oversight. Examining an agency's budget may help determine whether there is adequate investment in cyber-related areas or if adjustments are necessary to align with congressional expectations. Hearings, investigations, letters, speeches, and media appearances may help bring to light cybersecurity challenges facing the nation, the actions agencies are undertaking to address those challenges, and what (if any) gaps continue to exist that require additional legislation. Congress can also spur activity by directing agencies to develop strategies and reports. If additional legislation is necessary, Congress may choose to establish a program to address a particular facet of cybersecurity by authorizing an agency to do such work and appropriating funds for its execution.

Congress may also seek to achieve its cybersecurity goals by targeting the cybersecurity of firms operating in the United States. For instance, by establishing conditions for the use of technology; defining requirements for data privacy, retention, and use; incentivizing the behavior of companies either directly (e.g., through a grant program for critical infrastructure) or indirectly (e.g., by providing liability protections); or directing an industry to adopt standards, best practices, or participate in information sharing.

Chris Jaikaran, Specialist in Cybersecurity Policy

IF12851

Disclaimer