THIRD WAY

MEMO *Published February 10, 2021 • 13 minute read*

Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 116th Congress

Michael Garcia
Senior Policy Advisor
@garrrcya

Pat Shilo
Executive Coordinator
@Pat_Shilo

Takeaways

The 116th Congress experienced events like no other in American history, including unprecedented levels of malicious cyber activity. Global estimates say that ransomware attacks have increased by 148% since February 2020, with many US hospitals and schools falling victim and having their operations suspended.[1] Leading up to and during the pandemic, Members of the 116th Congress responded and drafted cybersecurity legislation, introducing 316 bills to tackle the issue—a 40% increase from the previous Congress.

This memo presents a comprehensive analysis of the cybersecurity legislation introduced in the 116th Congress and is a successor to our memo assessing the cybersecurity legislation in the previous Congress. Unlike the 115th Congress, the two chambers of the 116th were each

under the control of a different party. Still, more than half of the introduced bills were bipartisan, including 85% of the bills signed into law. However, only 11% of the introduced bills focused on imposing consequences for the human actors behind cyberattacks, such as imposing sanctions or strengthening laws to prosecute criminals to hold them accountable for their actions. Following the trend of past congresses, most of the bills focused on protecting data and securing critical infrastructure. But while defending data and infrastructure is important, the lack of legislation to address the challenges of imposing consequences on the human actor suggests that Congress should prioritize introducing and passing bipartisan legislation that reduces the impunity with which malicious cyber actors, particularly cybercriminals, act.

Here are the main takeaways from the bills introduced last Congress:

- Cybersecurity-related legislation increased by 40% since the 115th Congress.
- Of the 316 bills introduced, 14 became law, with nine related to appropriations or agency authorizations legislation.
- However, only 36 of the 316 bills introduced in the 116th Congress, and just three of the 14 provisions signed into law, focused on imposing consequences on the human actors behind cyberattacks.
- Cybersecurity remains a largely bipartisan issue. Over 50% of all legislation and 85% of all bills signed into law had a bipartisan co-sponsor.

Despite dealing with a global pandemic, the 116th Congress introduced 40% more cybersecurity legislation than the 115th Congress.

The COVID-19 pandemic exacerbated an already rising cybercrime wave in the United States that impacts all Americans. The Federal Bureau of Investigations (FBI) saw a 400% increase in the daily cybercrime incidents reported in April 2020 compared to their typical complaint rates. [2] Ransomware, too, increased 148% globally since February 2020, locking up and holding the data of US hospitals, schools, and small businesses for ransom in the midst of this global crisis. [3] Yet, the human actors behind these crimes are rarely punished. Our research shows that only three out of every 1,000 cyber incidents reported to the FBI result in an enforcement action. [4]

Before and during this crisis, Members of the 116 [th] Congress demonstrated an increased focus on the cyber threats facing our nation through their legislative action. In part, this is due to Congress'

introduction and approval of 26 of its over 60 recommendations made in the final report of the US Cyberspace Solarium Commission, which it authorized in the 115th Congress.[5] During the 116th Congress (January 3, 2019 – January 3, 2021), Members introduced 316 bills that either primarily or tangentially focused on cybersecurity.[6] To put this into context, Members introduced 13,481 bills in total, meaning that cyber-related legislation amounted to less than 3% of all introduced legislation.[7] However, the 116th Congress outpaced their predecessor, introducing 40% more cybersecurity bills than the 115th Congress.[8] Of these 316 bills, 93 were previously introduced in the 115th Congress, and five were signed into law. The increase in introduced cybersecurity legislation may be due to several reasons, such as an increased focus on the need to protect the 2020 elections from foreign interference, secure 5G and other supply chains from vulnerabilities, and counter the cyber threat posed by American adversaries.

The onset of COVID-19 also spurred legislation to protect user data that mobile applications for contact tracing may collect, such as the "COVID-19 Consumer Data Protection Act" (S.3663).[9] In fact, Members of Congress introduced at least 11 cyber-related bills in response to COVID-19, including some that would have imposed consequences on actors, like the "Defend COVID Research from Hackers Act" (S.4793).[10]

The House passed more cyber-related bills than their Senate colleagues, repeating a trend seen in the 115th Congress. The House passed 40 bills that the Senate did not pass, while the Senate passed eight bills that the House did not consider. This was par for the course compared to the 115th Congress, where the House passed 42 bills, and the Senate passed six.[11] Luckily, cybersecurity continued to be a bipartisan issue, with 55% of all legislation and 85% of all bills signed into law having bipartisan co-sponsors. This mirrored the bipartisanship seen in the 115th congressional session, where roughly 60% of all introduced bills had bipartisan cosponsors.

Of the 316 bills introduced, Congress passed 14 pieces of legislation into law. 65% of the bills signed into law were related to appropriations or authorizing an agency.[12] The table below details the name of these bills, their policy areas, and their sponsor.

Bill Name	Policy Area	Sponsor
CARES Act (H.R.748)	Appropriations	Joe Courtney
Consolidated Appropriations Act, 2019 (H.J.Res.31)	Appropriations	Lucille Roybal-Allard
Consolidated Appropriations Act, 2020 (H.R.1158)	Appropriations	Michael McCaul
Consolidated Appropriations Act, 2021 (H.R.133)	Appropriations	Henry Cuellar
Continuing Appropriations Act, 2021 and Other Extensions Act (H.R.8337)	Appropriations	Nita Lowey
Defending the Integrity of Voting Systems Act (S.1321)	Election Security	Richard Blumenthal
Further Consolidated Appropriations Act, 2020 (H.R.1865)	Appropriations	Bill Pascrell, Jr.
Internet of Things Cybersecurity Improvement Act (H.R.1668)	IoT	Robin Kelly
National Defense Authorization Act for Fiscal Year 2020 (S.1790)	Appropriations	James Inhofe
National Defense Authorization Act for Fiscal Year 2021 (H.R.6395)	Appropriations	Adam Smith
Pandemic and All-Hazards Preparedness and Advancing Innovation Act of 2019 (S.1379)	Appropriations	Richard Burr
Protecting Faith-Based and Nonprofit Organizations from Terrorism Act of 2019 (S.1539)	Other	Rob Portman
Secure 5G and Beyond Act of 2020 (S.893	Protecting Government/ Critical Infrastructure	John Cornyn
Taxpayer First Act (H.R.3151)	Breach Notification/ Consumer Protection	John Lewis

Source: Based on Third Way Research

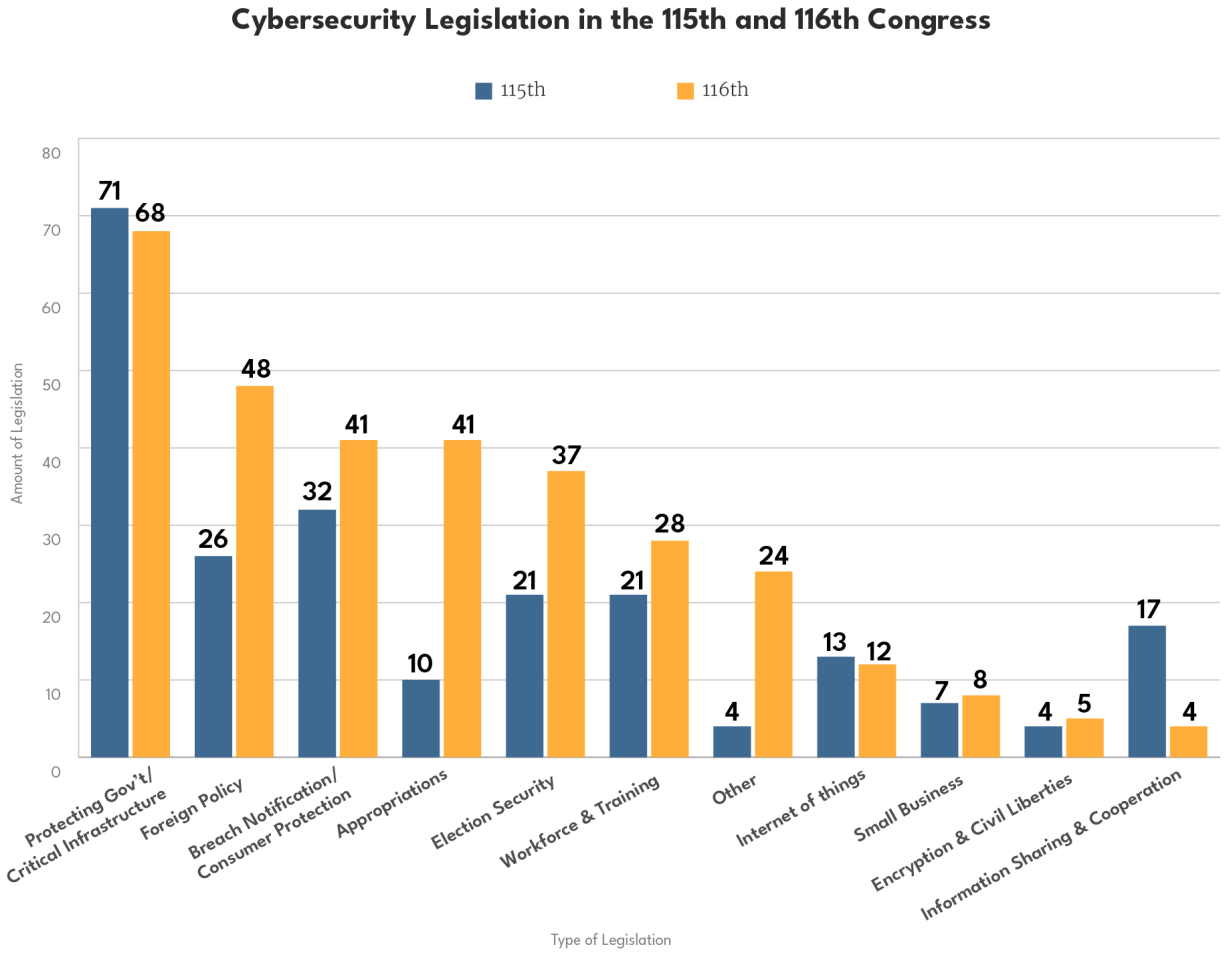
THIRD WAY

As the pandemic continues to rage and malicious cyber actors target vulnerable sectors, such as schools and hospitals, Members of Congress must continue introducing legislation that focuses on a range of cyber-related issues.

Most congressional cyber legislation focused on defending critical infrastructure, protecting consumer data, and advancing foreign policy priorities.

Examining the 316 bills introduced in the 116 th Congress shows the various cybersecurity issues Congress must contend with, ranging from protecting critical infrastructure to protecting consumer data held by third parties.

Half of the cyber-related bills introduced in the 116 th Congress dealt with defending critical infrastructure, protecting consumer data, and advancing foreign policy priorities—mirroring the 115 th 's top categories. The graph below compares the cyber-related legislation introduced by the two congressional sessions based on 11 thematic areas.



Source: Based on Third Way Research

Members introduced 68 bills that focused on protecting the federal government's networks or private critical infrastructure—the most of all 11 categories. These provisions included assisting state and local governments in defending their public networks, partnering with utility companies, and bolstering the Cybersecurity and Infrastructure Security Agency's (CISA) ability to defend federal networks. The "Secure 5G and Beyond Act of 2020" (P.L.116-129) was the only critical infrastructure bill signed into law., which requires the president to develop a strategy for securing and protecting US 5G infrastructure. [13] However, other bills, such as the "Cybersecurity Vulnerability Identification and Notification Act of 2020" (S.3045) which grants subpoena authority to CISA to notify private companies about a vulnerability, were included in larger appropriation and authorization legislation. [14]

The 116 th Congress also introduced 130 bills related to US foreign policy, breach notification/consumer protection, and appropriations, with Members introducing over 40 bills in each category. In terms of the latter, appropriation and authorization bills primarily focused on funding government agencies to protect their information technology systems or support their cybersecurity program areas. Yet, Members used these bills as vehicles to attach at least 45 cyber-

related bills. In fact, the two National Defense Authorization Acts (NDAA) passed by the 116 th Congress included 32 separate cyber-related bills.

Members of Congress introduced 48 cyber-related bills to advance foreign policy priorities, illustrating the international nature of cybersecurity and the need to strengthen global partnerships to address it. The 48 bills touched on various issues, such as bolstering countries' cybersecurity defenses and countering and imposing consequences on China, Russia, Iran, and North Korea's malicious cyber activities. In terms of the latter, Members introduced over 10 bills directed at the threat posed by China and Russia. For example, the "Advancing Competitiveness, Transparency, and Security in the Americas Act" (H.R.8716) sought to strengthen Latin American and Caribbean countries' criminal justice institutions to fight cybercrime in the region. [15]

The continued focus on consumer protection—tied for the third-highest category with appropriations—may be associated with Congress' interest in technology companies' roles and responsibilities in securing user's data from unauthorized disclosures.. For instance, the "Own Your Own Data Act" (S.806), the "Data Broker Accountability and Transparency Act of 2019" (S.2577), and the "Social Media Privacy Protection and Consumer Rights Act of 2019" (S.189), would have created security standards and limitations on the social media companies and data brokers that maintain user data. [16] Congress only passed one bill related to consumer protection, the "Taxpayer First Act" (P.L.116-25), enabling the Internal Revenue Service to work with private and public partners to protect taxpayers from identity theft fraud related to tax returns and strengthen other identity theft protection. [17]

Election security continued to be a top priority as well, with Members introducing 37 bills to bolster the cybersecurity of election infrastructure and combat online misinformation and disinformation. These bills included the "Bots Research Act" (H.R.2860), which would have directed the government to study the effects of automated accounts (i.e., bots) on social media, and the "ALERTS Act" (H.R.3529), which would have required the government to notify election officials of a breach into an election system. [18] But Congress only passed one election security bill - the "Defending the Integrity of Voting Systems Act" (P.L.116-179), which was one of the few bills that imposed consequences on malicious actors by making it a felony to hack a voting system. [19]

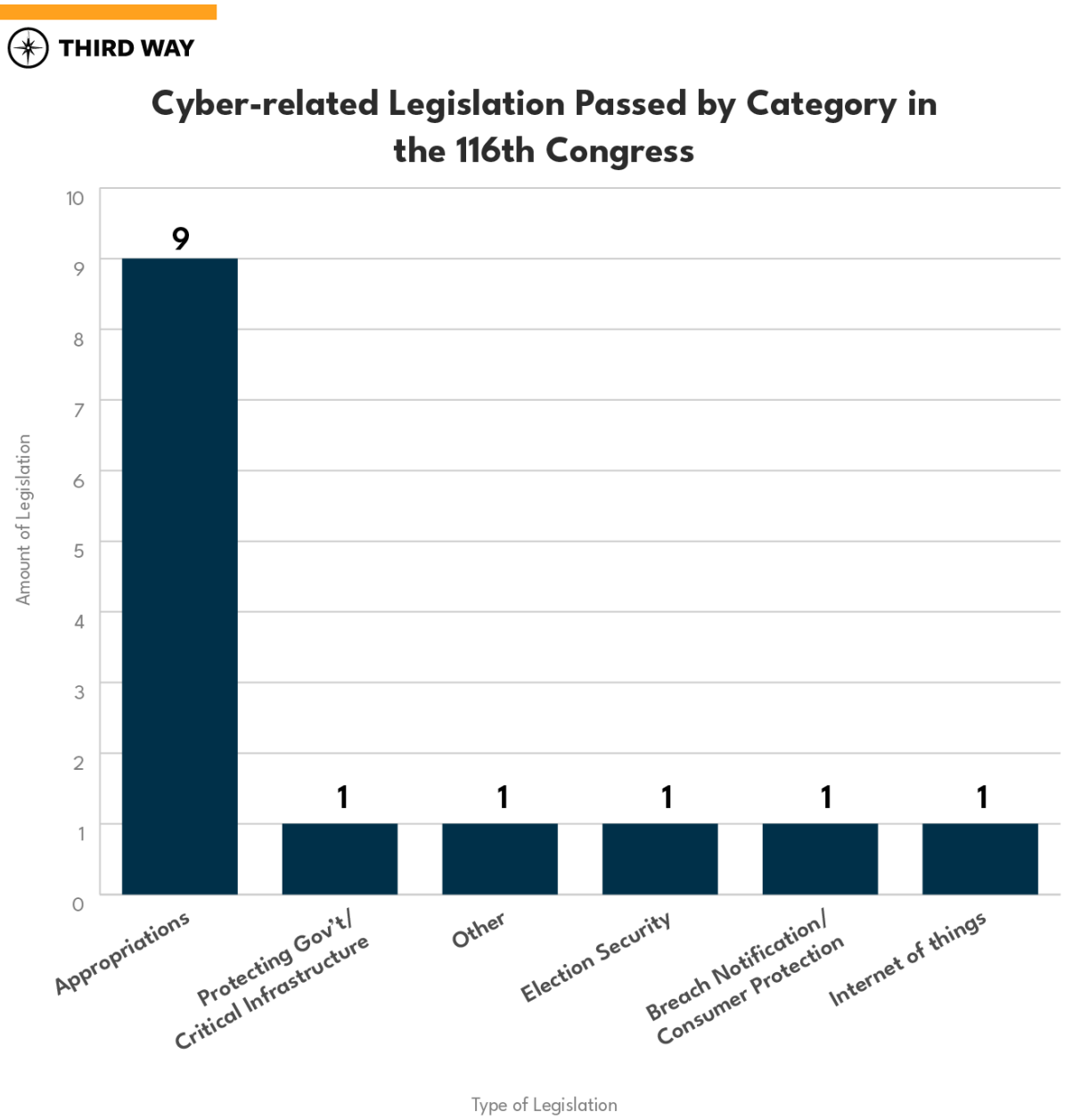
As technology becomes further engrained in everyday activities—from driverless cars to telehealth—the 117 th Congress will continue introducing and passing bills that touch on a wide range of issues.

Despite Congress' increased attention on cyber-related actions, a concerning gap remains in the legislative focus on cyber enforcement —

identifying, stopping, and imposing consequences on malicious cyber actors.

Although the 116 th Congress was highly active in introducing and passing cyber-related legislation, these provisions did little to impose consequences on the actors behind cyber incidents, such as cybercrime. While defending and protecting critical infrastructure and data remains important, Americans want to see their government reduce the rise of cybercrime. As mentioned earlier, only 3 in 1,000 cyber incidents reported to the FBI lead to an enforcement action. Yet, in a 2018 Statista poll, 72% of respondents worried that hackers would steal their personal, credit card, or financial information, placing this concern higher than having their car stolen or their home burglarized. [20] Further, 92% of respondents in a 2019 poll said that it was important for the next US president to make reducing cybercrime a top priority. [21]

Yet, only 36 of the 316 bills introduced and three of the bills signed into law dealt with imposing consequences on malicious actors, both nation-state and lone actors, who conducted malicious cyber activity, such as deploying ransomware—a form of cybercrime—against hospitals and schools. These bills included imposing sanctions, creating cyber enforcement strategies, improving criminal statutes, and providing resources to countries to apprehend the actor behind a cyber incident, such as cybercrime.



Source: Based on Third Way Research

Two of the three bills signed into law were the annual NDAAs, which further outlined the DoD's "defend forward" mission to monitor adversaries' networks and preemptively launch attacks to deter their malicious cyber activity. The third bill signed into law, "Defending the Integrity of Voting Systems Act" (P.L.116-179), makes it a felony to hack into an election system. [22] Several bills that were not signed into law would have taken significant steps to impose consequences on malicious actors but never gained traction. For example, the "Cyber Diplomacy Act of 2019" (H.R.739) would have established an ambassador for Cybersecurity and an elevated cyber office at the State Department but Congress did not approve it. [23] The "Technology in Criminal Justice Act of 2019" (H.R.5227), too, would have assisted state and local law enforcement close their cyber

enforcement gap by providing grants to improve their ability to analyze digital evidence left at the scene of a cybercrime. [24]

Improving critical infrastructure resilience to cyber attacks is highly important, but the ability to impose consequences against malicious actors and hold them accountable for their actions is also needed to deter malicious cyber activity. As the 117 th congressional session begins and after the wake of SolarWinds, the largest modern espionage attack on private and government systems, Members must consider legislation that deters these activities.

The 117th Congress can build off the bills introduced in the 116th congressional session to impose consequences and hold malicious cyber actors accountable.

As cyber actors continue to operate with near-impunity, they will continue to conduct cyber operations that impact everyday Americans, but the 117 th Congress can work to increase consequences on them for their actions. Members of Congress should focus their legislative effort on three key areas to hold malicious cyber actors accountable:

1. **Strengthening Ties with the Private Sector:** Since the private sector owns and operates the networks that malicious cyber actors abuse to perpetrate their attacks, the US government must continue collaborating with private partners to disrupt these actors' cyber networks and launch investigations into their actions. To this end, Congress should work with the newly authorized National Cyber Director to develop legislation that improves timely and actionable information sharing with private partners. [25]

2. **Fostering Global Cybercrime Cooperation**: As perpetrators of cyberattacks and crime are often located overseas, the US government must have the resources and authority to engage international partners to bring malicious actors to justice. We recommended in "A Roadmap to Strengthen US Cyber Enforcement," that Congress should prioritize reintroducing and passing the "Cyber Diplomacy Act of 2019" (H.R.739) to elevate a State Department cyber office in a chain-of-command that allows it to have cross-cutting authority. Congress must also provide funding to expand and evaluate bilateral and multilateral cyber capacity-building efforts around the globe. [26]

3. **Improving State and Local Cyber Enforcement**: Not every incident and crime will rise to the level that requires a federal response, and, like other crimes, state and local law enforcement will be called upon to respond in the absence of a federal response. Yet, the 18,000 law enforcement agencies in the United States lack the resources, tools, and personnel to respond effectively to cybercrime. Members of Congress should consider reintroducing the "Technology in Criminal Justice Act of 2019" (H.R.5227) and look to include additional provisions, such as those within the "Violence Against Women Reauthorization Act of 2019" (H.R.1585), to improve these agencies' capacities to fight cybercrime. [27]

Conclusion

The 117th Congress can build off the work of the 116th session's work and look to the 316 bills that were introduced for policy ideas, while also improving upon the 14 bills that were signed into law. Members should also focus on areas underrepresented in the 116th Congress, specifically measures that impose consequences on malicious cyber actors, while filling gaps in areas that received significant attention, like critical infrastructure resilience. Members of the 117th Congress will have a strong partner in President Biden—who has shown a willingness to work on bipartisan issues—to advance legislation that will close the cyber enforcement gap by strengthening relationships with private, local, and international partners.

TOPICS

CYBERSECURITY 72

ENDNOTES

1. Smith Malekos, Zhanna, et al. "The Hidden Costs of Cybercrime." *McAfee*, 7 Dec. 2020, pp. 25, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202. Accessed 23 Dec. 2020.

2. Peters, Allison and Garcia, Michael. "A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?" *Third Way*, 12 Nov. 2020, https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here. Accessed 23 Dec. 2020.

3. Smith Malekos, Zhanna, et al. "The Hidden Costs of Cybercrime." *McAfee*, 7 Dec. 2020, pp. 25, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202. Accessed 23 Dec. 2020.

4. Peters, Allison and Garcia, Michael. "A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?" *Third Way*, 12 Nov. 2020, https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here. Accessed 23 Dec. 2020.

5. Brumfield, Cynthia. "26 Cyberspace Solarium Commission recommendations likely to become law with NDAA passage." *CSO*, 14 Dec. 2020. https://www.csoonline.com/article/3601120/26-cyberspace-solarium-commission-recommendation-likely-to-become-law-with-ndaa-passage.html Accessed 12 Jan. 2021.

6. For the purpose of this memo we have relied on the Congressional Research Service's classification to define "cybersecurity legislation." This includes legislation focused on offensive, defensive, and enforcement. It does not include legislation that solely focuses on other digital/cyber issues like privacy, net neutrality, and Internet Access.

7. Quorum Analytics. "Congress on Social Media 2020." *Quorum Analytics*, pp. 3, Dec. 2020. https://www.quorum.us/wp-content/uploads/2020/12/Quorum_Report_CongressOnSocialMediaFINAL.pdf. Accessed 23 Dec. 2020.

8. Mehta, Ishan and Dev, Jayati. "Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 115th Congress." *Third Way*, 21 Feb. 2019, https://www.thirdway.org/memo/taking-action-on-cyber-enforcement-assessing-us-legislative-progress-in-the-115th-congress. Accessed 23 Dec. 2020.; Tehan, Rita. "Cybersecurity: Legislation, Hearings, and Executive Branch Documents." *Congressional Research Service*, 8 Nov. 2018, https://fas.org/sgp/crs/misc/R43317.pdf. Accessed 23 Dec. 2020.

9. United States, Congress, Senate. COVID-19 Consumer Data Protection Act of 2020. *Congress.gov*, https://www.congress.gov/bill/116th-congress/senate-bill/3663. 116 th Congress, 2 nd session, introduced 7 May 2020.

10. United States, Congress, Senate. Defend COVID Research from Hackers Act. https://www.congress.gov/bill/116th-congress/senate-bill/4793/text?r=1&s=1. 116 th Congress, 2 nd session, introduced 1 Oct. 2020.

11. Mehta, Ishan and Dev, Jayati. "Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 115th Congress." *Third Way*, 21 Feb. 2019, https://www.thirdway.org/memo/taking-action-on-cyber-enforcement-assessing-us-legislative-progress-in-the-115th-congress.

12. All authorization bills were cataloged as "appropriations" to remain consistent with the categories used in the "Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 115 th Congress."

13. United States, Congress, Senate. Secure 5G and Beyond Act of 2020. *Congress.gov*, https://www.congress.gov/116/plaws/publ129/PLAW-116publ129.pdf. 116th Congress, 1st session, Public Law 116-129, signed into law 23 March 2020.

14. United States, Congress, Senate. Cybersecurity Vulnerability Identification and Notification Act of 2020. *Congress.gov*, https://www.congress.gov/bill/116th-congress/senate-bill/3045?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=38&s=1. 116th Congress, 1st session, Senate Resolution 3045, introduced 12 Dec. 2019.

15. United States, Congress, House. Advancing Competitiveness, Transparency, and Security in the Americas Act of 2020. *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/8716?s=1&r=1. 116th Congress, 2nd session, House Resolution 8716, introduced 30 Oct. 2020.

16. United States, Congress, Senate. Own Your Own Data Act. *Congress.gov*, https://www.congress.gov/bill/116th-congress/senate-bill/806. 116th Congress, 1st session, Senate Resolution 806, introduced 14 March 2019.; United States, Congress, Senate. Data Broker Accountability and Transparency Act of 2019. *Congress.gov*, https://www.congress.gov/bill/116th-congress/senate-bill/2577?q=%7B%22search%22%3A%5B%22DATA PROTECTION%22%5D%7D&s=1&r=321. 116th Congress, 1st session, Senate Resolution 2577, introduced 26 Sept. 2019.; United States, Congress, Senate. Social Media Privacy Protection and Consumer Rights Act of 2019. *Congress.gov*, https://www.congress.gov/bill/116th-congress/senate-bill/189. 116th Congress, 1st session, Senate Resolution 189, introduced 17 Jan. 2019.

17. United States, Congress, House. Taxpayer First Act. *Congress.gov*, https://www.congress.gov/116/plaws/publ25/PLAW-116publ25.pdf. 116th Congress, 1st session, Public Law 116-25, signed into law 1 July 2019.

18. United States, Congress, House. Bots Research Act. *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/2860/text?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=88&s=3. 116th Congress, 1st session, House Resolution 2860, introduced 21 May 2019; United States, Congress, House. Achieving Lasting Electoral Reforms on Transparency and Security Act. *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/3529/text. 116th Congress, 1st session, House Resolution 3529, introduced 27 June 2019.

19. United States, Congress, Senate. Defending the Integrity of Voting Systems Act. *Congress.gov*, https://www.congress.gov/116/plaws/publ179/PLAW-116publ179.pdf. 116th Congress, 1st session, Public Law 116-179, signed into law 20 Oct. 2020.

20. "Crimes Americans Worry About Most in 2019." *Statista*, 11 Dec. 2019. www.statista.com/statistics/339735/crime-worries-in-the-united-states/. Accessed 17 Oct. 2020.

21. Mehta, Ishan. "Poll Shows Voters Want Next President to Make Reducing Cybercrime a Top Priority." *Third Way*, 1 Oct. 2019, www.thirdway.org/blog/poll-shows-voters-want-next-president-to-make-reducing-cybercrime-a-top-priority. Accessed 23 Dec. 2020

22. United States, Congress, Senate. Defending the Integrity of Voting Systems Act. *Congress.gov*, https://www.congress.gov/116/plaws/publ179/PLAW-116publ179.pdf. 116th Congress, 1st session, Public Law 116-179, signed into law 20 Oct. 2020.

23. United States, Congress, House. Cyber Diplomacy Act of 2019. *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/739/text?q=%7B%22search%22%3A%5B%22cyber OR influence OR cybercrime or electronic or data%22%5D%7D&r=2&s=3. 116th Congress, 1st session, House Resolution 739, introduced 1 Jan. 2019.

24. United States, Congress, House. Technology in Criminal Justice Act of 2019. *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/5227?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&s=2&r=175. 116th Congress, 1st session, House Resolution 5227, introduced 21 Nov. 2019.

25. For examples on the National Cyber Director can strengthen relations with the private sector, please see https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here

26. On January 7, 2021, Secretary of State Mike Pompeo approved the creation of the Bureau of Cyberspace Security and Emerging Technologies. However, Members of Congress have raised concerns about how the Trump Administration is moving forward with the Bureau. US House of Representatives, Committee on Foreign Affairs. "Meeks Statement on State Department Cyber Bureau." 7 Jan 2021. https://foreignaffairs.house.gov/2021/1/meeks-statement-on-state-department-cyber-bureau. Accessed 12 Jan 2021 and Peters, Allison and Garcia, Michael. "A Roadmap to strengthen US Cyber Enforcement: Where Do We Go From Here?" *Third Way*, 12 Nov. 2020, p.45 https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here#:~:text=From%20April%20to%20October%202020,recommendations%20on%20cyber%20enforcement%20for Accessed 12 Jan 2021.

27. United States, Congress, House. Technology in Criminal Justice Act of 2019. *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/5227?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&s=2&r=175. 116th Congress, 1st session, House Resolution 5227, introduced 21 Nov. 2019; United States, Congress, House. Violence Against Women Reauthorization Act of 2019. *Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/1585/text#toc-H41DAA9F60FE84F0C94ED39F2D89535D8. 116th Congress, 1st session, House Resolution 1585, passed 4 Apr. 2019.