Michael Kans' Technology Policy Update
24 May 2019
By Michael Kans, Esq.

Targeted Cyber Legislation Marked Up

This week, a number of committees marked up and reported out targeted cybersecurity bills, some of which should be taken up by their respective chambers in the next few months. A number of these bills advanced through one body in the last Congress but failed to gain traction in the other for a variety of reasons.

The House Homeland Security Committee marked up and reported out the "DHS Cyber Incident Response Team Act" (H.R. 1158). Sponsor Michael McCaul (R-TX) stated:

> [The bill] is an innovative and strong addition to ensuring we have an important mechanism to respond to cyber incidents…[and] ensures that the Department of Homeland Security (DHS) has cyber incident response teams to aid federal agencies and the private sector in identifying, responding to, and mitigating cybersecurity threats." These teams assist compromised cyber-assets with response efforts and provide recommendations for improving networks. Furthermore, this legislation enables DHS to foster collaboration between the public and private sector by allowing specialists to operate on cyber incident response teams that maximize our efforts to combat cyber threats.

A similar bill was passed by the House last year but never considered by the Senate.

On May 16, the Senate Judiciary Committee held a markup and approved two bills by voice vote:

- The "Defending Elections against Trolls from Enemy Regimes (DETER) Act" (S. 1328), introduced by Senator Dick Durbin (D-IL), which would amend the "Immigration and Nationality Act" (8 USC 1101) by allowing U.S. officials to deny admission to the U.S. of any foreign person for which there are reasonable grounds he or she conducted "improper interference in a United States election."
- The "Defending the Integrity of Voting Systems Act" (S. 1321), introduced by Senator Richard Blumenthal (D-CT), that would amend the "Computer Fraud and Abuse Act" (18 USC 1030) by adding interference with voting systems as a prohibited activity. Specifically, the bill would bar the interference with any "part of a voting system…used for the management, support, or administration of a Federal election."

Also, on May 16, the House Energy and Commerce Committee's Energy Subcommittee marked up four cyber-related bills and forwarded them to the full committee by voice vote:

- The "Enhancing Grid Security through Public-Private Partnerships Act" (H.R. 359)
- The "Cyber Sense Act of 2019" (H.R. 360)
- The "Energy Emergency Leadership Act" (H.R. 362)
- The "Pipeline and LNG Facility Cybersecurity Preparedness Act" (H.R. 370)

Committee Democrats summarized the four bills:

- H.R. 359 directs the Secretary of Energy, in consultation with States, other Federal agencies, and industry stakeholders, to create and implement a program to enhance the physical and

cyber security of electric utilities. Among other things, this program would develop voluntary implementation of methods for assessing security vulnerabilities. It would provide cybersecurity training to electric utilities, advance the cybersecurity of utility third-party vendors, and promote sharing of best practices and data collection in the electric sector. The bill requires DOE to submit a report to Congress on cybersecurity and distribution systems.

- H.R. 360 requires the Secretary of Energy to establish the Cyber Sense Program. This voluntary program would identify cyber-secure products that could be used in the bulk-power system. In addition to making DOE responsible for promoting cyber-secure products, this legislation requires DOE to determine a testing process for Cyber Sense products and establish a cybersecurity vulnerability reporting process and database.
- The legislation amends Section 203(a) of the Department of Energy Organization Act to create a new DOE Assistant Secretary position with jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity. The bill authorizes the new Assistant Secretary to provide, upon request of a State, local, or tribal government, DOE with technical assistance, and support and response capabilities with respect to energy security threats, risks, and incidents.
- H.R. 370 would establish a program at DOE, in coordination with other Federal agencies, States, and the energy sector, to create policies and procedures that would improve the physical and cyber security and resiliency of natural gas transmission and distribution pipelines, hazardous liquid pipelines, and liquefied natural gas (LNG) facilities. The Secretary of Energy would coordinate responses to, and recovery from, physical and cyber incidents affecting the energy sector and develop advanced cybersecurity technologies, perform pilot demonstration projects, and establish workforce development security curricula for pipelines and LNG facilities. Finally, the bill would provide mechanisms to help the energy sector evaluate, prioritize, and improve security capabilities for such facilities.

On May 14, the Senate Intelligence Committee marked up and reported out the "Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act (IAA) for Fiscal Years 2018, 2019, and 2020" (S. 1589) by a 15-0 vote. In its press release, the Committee highlighted some of the cybersecurity-related portions of the bill:

- Countering aggression from Russia and other foreign actors by increasing our capabilities to detect Russian activities, including active measures campaigns, illicit financial transactions, and other intelligence activities.
- Securing our elections from foreign meddling by requiring strategic assessments of Russian cyber threats and influence campaigns, and facilitating increased information sharing between state, local, and federal government officials.
- Improving the security clearance process by requiring a plan to reduce the backlog, increase efficiencies, create an interagency information sharing program for positions of trust, and ensure compliance with uniform clearance eligibility procedures within the Federal government.
- Protecting the U.S. Government technology supply chain by creating a task force within the Office of the Director of National Intelligence and improving the procurement process to defend against intrusion and sabotage.
- Bolstering the recruitment and retention of science, technology, engineering and math (STEM) professionals by enhancing career path flexibility and benefits for cybersecurity experts working within the Intelligence Community.

5G Hearing

On May 14, the Senate Judiciary Committee held a hearing titled "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation." This hearing represents this committee's continued interest in helping to shape policy on technology issues with a national security facet.

The committee heard from two panels of witnesses:

Panel I

- Cybersecurity and Infrastructure Security Agency Director Christopher Krebs
- Deputy Assistant Secretary of States for Cyber and International Communications and Information Policy Robert Strayer

Panel II

- Center for Strategic and International Studies Senior Vice President Dr. James A. Lewis, Ph.D.
- Virginia Polytechnic Institute and State University's Hume Center for National Security and Technology Executive Director Dr. T. Charles Clancy, Ph.D.
- Center for a New American Security Adjunct Senior Fellow Peter Harrell

Chairman Lindsey Graham (R-SC) said that he was interested in learning what the development of 5G networks will mean for the average American consumer, the U.S., and its allies. He stated that we was looking forward to learning about the issue and hearing how Congress could help solve whatever problems there may be.

Ranking Member Dianne Feinstein (D-CA) said she has been told that 5G would fundamentally change U.S. society , economy, and national security, hence the need for understanding the issue. She said 5G is touted as having the ability to provide exponential increases in speed, capacity, and reliability for all internet-connected devices, which would bring forth a variety of revolutionary technologies. Feinstein quoted Federal Bureau of Investigation (FBI) Director Christopher Wray who said that 5G has the capacity to exert pressure or control over our telecommunications infrastructure, to maliciously modify or intercept information, and conduct undetectable espionage. She said there is fierce competition between nations in the 5G market and noted the $400 billion spent by the Chinese government and related efforts to shape and influence the rollout of 5G. Feinstein said that Huawei has grown very quickly and holds 28% of the global market. Feinstein said the requirements placed on Chinese companies by their government is the key issue, notably the 2017 intelligence law that mandates that all companies assist and cooperate with Chinese's intelligence agencies.

Krebs stated

> During his annual Worldwide Threat Assessment testimony before Congress this January, the Director of National Intelligence stated, "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies." The Director further stated, "We are also concerned about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies." This assessment is consistent with the fact that Chinese laws on national

security and cybersecurity provide the Chinese government with a legal basis to compel technology companies operating in China to cooperate with Chinese security services.

Krebs noted that "[t]he concern regarding the growing presence of Chinese telecom equipment is particularly acute in the Radio Access Network (RAN) portion of the network where there are a limited number of RAN equipment suppliers." He said that "[t]here are four main purveyors of 5G RAN technology globally, none of which are considered United States-based, and the largest of which is Chinese-based." Krebs stated that "[i]f Chinese manufacturers, who receive significant state support, continue to gain market share, there will be growing concern about the long-term viability of the existing supply chain for 5G and successor technologies."

Krebs stated that "[r]isks to mobile communications generally include such activities as call interception and monitoring, user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data." He asserted that "[i]ntegrating 5G into current wireless networks may convey existing vulnerabilities and impact 5G network security. Data on 5G networks will flow through interconnected cellular towers, small cells, and mobile devices that may provide malicious actors additional vectors to intercept, manipulate, or destroy critical data." Krebs said that "[m]alicious actors could also introduce device vulnerabilities into the 5G supply chain to compromise unsecured wireless systems and exfiltrate critical infrastructure data."

Strayer stated that "[a]s countries around the world upgrade their communications systems to 5G technology, we are urging them to adopt a risk-based security framework." He explained that "[t]o this end, the Department is executing a global campaign on 5G security that includes strategic bilateral and multilateral engagements to convince our allies and partners of the seriousness of the need to adequately secure these networks." Strayer stated that "[a]n important element of this risk-based security approach is a careful evaluation of hardware and software equipment vendors and the supply chain." He asserted that "[t]he evaluation criteria should include the extent to which vendors are subject to control by a foreign government with no meaningful checks and balances on its power to compel cooperation of these vendors with its intelligence and security agencies." Strayer said that "[f]or example, because of the essential role that vendors play in networks and their maintenance, they could be ordered to undermine network security—to steal personal information or intellectual property, conduct espionage, disrupt critical services, or conduct cyber attacks."

Strayer stated that "Chinese technology firms are already working with authoritarian regimes – often hand-in-hand with the Chinese government – to suppress freedom of expression and other human rights through arbitrary surveillance, censorship, and targeted restrictions on Internet access." He contended that "[i]f Chinese companies build the underlying 5G infrastructure, they will be in an even better position to facilitate these activities." Strayer added that "China has a long history of undertaking intellectual property theft to benefit its commercial interests…[and]…[c]ountries should not allow 5G to be another vector for China to steal their intellectual property." He claimed that "Chinese companies, such as Huawei, appear to have benefited from subsidized financing for their equipment sales…[and] [c]ountries should adopt the best practices in procurement, investment, and contracting, and require that financing be commercially reasonable, conducted openly and transparently, and based on free market competitive principles, while taking into account trade obligations."

ICT Executive Order

On May 15, the Trump Administration released a long anticipated executive order (EO) aimed at China's technology industry, notably at its 5G capabilities. The EO titled "Securing the Information and Communications Technology and Services Supply Chain" is intended "to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States" through the declaration of a national emergency. The EO would bar U.S. entities from buying or using the information and communications technology and services (ICT) from "foreign adversaries" if a determination is made that doing so would sabotage or subvert U.S. ICT, place U.S. critical infrastructure or its digital economy at "undue risk," or "poses an unacceptable risk" to national security or safety. The only "foreign adversary" that is positioned to threaten the U.S. in this fashion is China through Chinese companies such as Huawei, ZTE, and others that supply key goods to the supply chain of international technology firms and offers their own devices and services. It is likely that the EO is seen by the White House as a bargaining chip with China in negotiations on trade and tariffs and, as such, may never come fully into force as the Secretary of Commerce will receive discretion to modify the blanket ban on Chinese information and communications technology and services. Last year, the Department of Commerce replaced the seven-year ban on ZTE with $1 billion in sanctions at the behest of the President who tweeted his concern that the ban would result in too many lost jobs in China.

In relevant part, the EO bars the "acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service" if the Department of Commerce "has determined that:

> (i) the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
> (ii) the transaction:
>> (A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
>> (B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
>> (C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

However, the Department of Commerce "may at the Secretary's discretion design or negotiate measures to mitigate concerns…[and] [s]uch measures may serve as a precondition to the approval of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order."

The Department of Commerce must issue regulations putting into effect this EO within 5 months. The agency is also "authorized to take such actions, including directing the timing and manner of the cessation of transactions prohibited…adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA, as may be necessary to implement this order."

Hearing on "China's Digital Authoritarianism"

On My 16, the House Intelligence Committee held a hearing titled "China's Digital Authoritarianism: Surveillance, Influence, and Political Control." Both Democrats and Republicans expressed concern about how advanced technologies are being used in China and elsewhere to stifle basic freedoms

and how these Chinese initiatives fit into the country's larger strategy to displace the U.S. as the world's preeminent power. Members and witnesses discussed at some length how many of these same surveillance techniques might inform Chinese espionage against the U.S. and its allies. The witnesses urged Congress and the Administration to establish a comprehensive U.S. strategy to counter the rise of this new authoritarianism and the threat China poses to the established world order. However, while there is bipartisan concern and desire to effect policy changes, it is not clear how far this consensus reaches.

The witnesses appearing before the committee were:

- Australian Strategic Policy Institute's International Cyber Policy Centre Non-Resident Fellow Dr. Samantha Hoffman
- Victims of Communism Memorial Foundation Research Fellow in China Studies Peter Mattis
- Cornell University Professor Dr. Jessica Chen Weiss
- National Endowment for Democracy Vice President Christopher Walker

Chairman Adam Schiff (D-CA) said the "hearing is part of our committee's broader effort to understand this trend's impact on the Intelligence Community and broader national security interests of the United States…[and] is also the formal launch of our committee's deep dive on China this session, where we will continue to look at issues in open and closed session for the duration of the 116th Congress." He said "[t]oday, our Nation faces no greater long-term strategic challenge than China's emergence as a major actor on the global stage." Schiff said that "[c]itizens of China today live their lives bounded by the guardrails of ubiquitous surveillance and pervasive influence operations, all in the name of the Chinese Communist Party's desire to retain political control." He said that "[l]everaging advances in artificial intelligence, machine learning, and facial recognition software, Beijing seeks to optimize and cement the social control of its population." He asserted that the "coupling of information and authoritarianism is deeply troubling and has spread beyond China itself." He stated that "Huawei's so-called safe cities have been installed in at least 46 countries…[and] [t]hese systems link 24/7 surveillance with command and control centers, facial and license plate recognition technologies, data labs, and intelligence fusion capabilities." Schiff stated that "[t]his export of technology gives countries the technological tools they need to emulate Beijing's model of social and political control…[and] [t]hese technologies have not only enabled China's quest to gain market share, they are also shaping the world in a way that also encourages support for their brand of governance and restrictions on personal liberty."

Ranking Member Devin Nunes (R-CA) stated that "I hope our discussion will draw attention to Chinese adoption and exportation of invasive surveillance measures designed to optimize political control, as well as Beijing's overseas influence operations targeting the U.S. and Five Eyes governments, including activities directed by Chinese Communist Party's United Front Work Department." He contended that "[i]t is important that we better understand what the Chinese Communists are doing because Beijing has implemented an aggressive and sophisticated whole-of-society influence campaign to win supporters, sow confusion in the American public, and undermine opposition to the Chinese threat within American society." Nunes claimed that "[t]oday's open hearing continues this committee's years-long initiative on China." He added that "[t]he committee's views on the malign activities of Huawei and ZTE reflected in our 2012 publicly available report and last year's unclassified report titled "Committee's Review on China's Malign Activities and the Intelligence Community's Response" provides important additional information for understanding the China threat." Nunes stated that "[l]ooking forward, this committee needs to continue to explore the vast array of Chinese efforts to threaten American interests, including talent recruitment, academic exchanges, and Beijing's activities, both legal and illicit, to acquire critical national

security technologies and intellectual property." He asserted that "[i]n the last Congress, the Democrats focused disproportionate attention on false allegations that Trump associates colluded with Russia to hack the 2016 election, even interrupting an open hearing on China to demand a subpoena related to their Russia collusion theory. " Nunes stated that "I hope, in this Congress, the committee will pay appropriate attention to the true array of threats emanating from Beijing and other bad actors worldwide."

Hoffman offered "a few key observations:

1) The United States and other liberal democracies have massively underestimated what China would do with its vision to use technology to augment its authoritarianism. What we are seeing now is a manifestation of plans already in place and in fact public for years, even decades. We are still underestimating their potential.
2) The Chinese Communist Party (CCP) uses technology to make its Gordian knot of political control inseparable from China's social and economic development. The CCP's construction of the social credit system and development of smart cities are the embodiment of this strategy, allowing the CCP to blur the line between cooperative and coercive control.
3) Technology already allows the CCP to expand its power in ways we have not been prepared to think about previously. The issue can only be framed through the CCP's concept of state security, which places political security and ideological security at its core. The concept is not about protecting China and the Chinese people separately from the Party's leadership.
4) To guarantee state security, the CCP prioritizes expanding its power. The CCP's "state security" strategy implies that the scale of the challenge is much larger than the scope of current debate. The U.S. is not simply managing a threat to national security, but also to long-term economic stability, security and the protection of civil liberties.
5) The CCP's power-expansion effort does not stop at China's geographic borders, largely because state security strategy is driven by the Party's political and ideological core. The CCP aims to re-shape global governance. It attempts to control international discourse on China and the channels through which individuals, businesses, and governments, can engage with China. It expects technology to enhance the sophistication of this process."

Mattis stated that "[h]ere are a few of the ways in which the Chinese Communist Party has shaped the ways in which Americans discuss, understand, and respond to the People's Republic of China, its rise, and its activities:

- We have been persuaded that the Chinese Communist Party is not ideological and has substituted its Leninist tradition for a variation of capitalism.
- We have not responded to violence, coercion, and intimidation committed or instigated by PRC officials on U.S. soil. These are allegedly criminal acts committed by a foreign government against our people on our soil, and U.S. authorities did not open criminal investigations.
- We have not responded to PRC education officials intimidating Chinese students on university campuses, despite this activity not being consistent with their diplomatic status.
- We have changed our laws at the state level to facilitate the Confucius Institute program to help the party build beachheads inside universities.
- We often debate our policy options toward China in binary terms: engagement vs containment; trade war or negotiation; accommodation or war; etc."

Walker said that "[t]he following are key steps, drawn from our Sharp Power report, which can be taken to address the Beijing's influence efforts:

- Address the evident knowledge and capacity gap on China. Throughout many societies in which China today is deeply engaged information concerning the Chinese political system and its foreign policy strategies tends to be extremely limited. This places many societies at a distinct strategic disadvantage. There often are few journalists, editors, and policy professionals who possess a deep understanding of China—the Chinese Communist Party, especially—and can share their knowledge with the rest of their societies in a systematic way. Given China's growing economic, media, and political footprint in these settings, there is a pressing need to build capacity to disseminate independent information about China and its regime. Civil society organizations should develop strategies for communicating expert knowledge about China to broader audiences.
- Shine a spotlight on authoritarian influence. Chinese sharp power relies in part on disguising state-directed projects as commercial media or grassroots associations, for example, or using local actors as conduits for foreign propaganda or tools of foreign manipulation. To respond to these efforts at misdirection, observers need the capacity to put them under the spotlight and analyze them in an independent and comprehensive manner.
- Safeguard democratic societies against undesirable Chinese Party State influence. Once the nature and techniques of authoritarian influence efforts are exposed, countries should build up internal defenses. Authoritarian initiatives are directed at cultivating relationships with the political elites, thought leaders, and other information gatekeepers of open societies. Such efforts are part of Beijing's larger aim to get inside such systems in order to incentivize cooperation and neutralize criticism of the authoritarian regime. Support for strong, independent civil society—including independent media—is essential to ensuring that the citizens of democracies are adequately informed to evaluate critically the benefits and risks of closer engagement with Beijing and its surrogates. It is impossible to know for certain, for instance, the degree to which intimidation from authoritarian governments has already made scholars and publishers "sensitive-topic averse." Exposing the hidden pressures is a first step toward countering the censors' insidious influence.
- Reaffirm support for democratic values and ideals. If one goal of authoritarian sharp power is to legitimize nondemocratic forms of government, then it is only effective to the extent that democracies and their citizens lose sight of their own principles. The Chinese government's sharp power seeks to undermine democratic standards and ideals. Top leaders in the democracies must speak out clearly and consistently on behalf of democratic ideals and put down clear markers regarding acceptable standards of democratic behavior. Otherwise, the authoritarians will fill the void.
- Learn from democratic partners. A number of countries, Australia especially, have already had extensive engagement with China and can serve as an important point of reference for countries whose institutions are at an earlier stage of their interaction with Beijing. Given the complex and multifaceted character of Beijing's influence activities, such learning between and among democracies is critical for accelerating responses that are at once effective and consistent with democratic standards."

Senate Rules Committee Hearing on Election Security

On May 15, the Senate Rules and Administration Committee conducted an oversight hearing of the Election Assistance Commission (EAC), but there was no indication that committee Republicans were ready to move election security legislation. Despite passage of a House bill to bolster the cybersecurity of U.S. election systems, Senate Republicans and the White House to show scant interest in similar legislation coming to the Senate floor. Nonetheless, Democrats in both chambers continue to push legislation, for they see it as a vital step to ensure that Russia and other adversarial

nations do not interfere with or influence the 2020 Presidential election as they did in the 2016 election. It is possible that very narrow legislation gets moved in the Senate, or that the EAC receives additional funds for election security in FY 2020 as they did in in FY 2018, however.

Chair Roy Blunt (R-MO) stated that "the Election Assistance Commission (EAC) plays an important role in assisting state and local election officials' efforts to provide an accessible and secure election process." He stated that "[l]ast Congress, we heard from the EAC about the distribution of $380 million in ["Help America Vote Act" (P.L. 107-252)] grant money that was included in the FY 2018 spending bill and about the agency's other efforts to assist state and local election officials, especially those related to ensuring that those officials received timely and accurate cybersecurity threat information." Blunt noted that "[l]ast Congress, this Committee also approved and the Senate confirmed two new EAC Commissioners, giving the EAC a full slate of commissioners for the first time in nearly 10 years and a quorum after nine months without one." He contended that "[t]oday, with four EAC Commissioners in place, we will hear about the progress of updating the voluntary voting systems guidelines, the agency's work to ensure that election officials around the country have the information they need to ensure the security of our nation's elections and the EAC's preparedness for the 2020 elections." He said that "[a]s I have mentioned before, I believe the EAC has an important role to play, given the changing landscape of elections in this country and the increase in cyber threats to elections…[and] I look forward to hearing from the Commissioners today about how the EAC will meet these challenges."

Ranking Member Amy Klobuchar (D-MN) stated that it is vital that the EAC, Congress, and other stakeholders work together on a bipartisan basis because "election security is our country's security" and everyone wants to be sure U.S. elections are free of foreign influence. She stated that recent news that Russian hackers accessed elections systems in two Florida counties demonstrates that the interference in 2016 is real and requires a united front. Klobuchar stated that these threats show why the EAC, the only federal agency whose sole mission is to improve elections, is so important. She contended that Russia invaded the U.S.' democracy but did not use guns, missiles, or tanks. Klobuchar quoted Special Counsel Robert Mueller's assertion that Russian interference was undertaken in a sweeping and systemic fashion, including sophisticated influence operations. She noted that Trump Administration intelligence officials continue to warn that U.S. elections remain a target of influence campaigns. Klobuchar claimed there are "a common set of facts about what happened and we know there's a continued threat." She said that what policymakers need to do now is to determine how to address this situation with a common purpose and prepare for the next election. Klobuchar claimed that at least 40 states rely on electronic voting systems more than 10 years old, and 12 states either do not use paper ballots or have no backup system. She stated that states have spent about 30% of the $380 million made available for election security, and she characterized these funds "as a good start" but a fraction of what an aircraft carrier costs. Klobuchar expressed disappointment that the "Elections Security Act" (S. 2593) did not advance to the floor in the last Congress and called for the Senate to consider this bill.

EAC Chair Christy McCormick said that "[E]lection security is a theme that continues to shape the national conversation about election administration, especially as we look ahead to 2020." She noted that "[f]ederal law enforcement and intelligence officials regularly remind us that the threats election administrators faced in 2016 and 2018 remain today and are likely to intensify in the months and years ahead." McCormick stated that "[w]e take seriously the fact that voter confidence is enhanced when we adequately prepare for and respond to challenges such as election misinformation campaigns, persistent attempts to breach elections systems and voter registration databases, and other real threats." She said the EAC has taken a "multifaceted approach to helping

state and local election officials strengthen their election security…[which] includes testing and federally certifying voting systems, providing hands-on security and post-election audit trainings across the country, producing security-focused resources, disseminating security best practices information and checklists to state and local election officials, as well as hosting widely attended forums that feature security experts as speakers." McCormick stated that the "EAC will continue to meet the requirements of HAVA…[but] without additional resources, it will be a formidable stretch for our capable, devoted staff members who already work tirelessly to support our nation's election administrators and voters."

Earlier in the week, Klobuchar and other Senate Democrats introduced the "Election Security Act" (S. 1540), the Senate version of the stand-alone measure introduced in the House that was taken from the larger package, the "For the People Act" (H.R. 1) passed by the House earlier this year the Senate will not take up.

According to their press release, the sponsors claimed "The Election Security Act would:

- Require states use paper ballots.
- Establish cybersecurity standards for voting systems vendors.
- Fund grants for states to improve and maintain the security of their election systems, to provide cybersecurity training to election officials, and to implement post-election risk limiting audits.
- Require the [Director of National Intelligence] to assess threats to election systems 180 days before an election and require [Department of Homeland Security] and the Election Assistance Commission to issue recommendations to address threats.
- Require the testing of voting systems nine months before an election.
- Require the President to produce a national strategy for protecting democratic institutions.
- Create a National Commission to Protect United States Democratic Institutions.

In August 2018, the Senate Rules and Administration Committee postponed indefinitely a markup on a compromise bill to provide states additional assistance in securing elections from interference, the "The Secure Elections Act" (S.2593). Reportedly, there was concern among state officials that a provision requiring audits of election results would be in effect an unfunded mandate even though this provision was softened at the insistence of Senate Republican leadership. However, a White House spokesperson indicated in a statement that the Administration opposed the bill, which may have posed an additional obstacle to Committee action. However, even if the Senate had passed its bill, it was unlikely that the Republican controlled House would have considered companion legislation (H.R. 6663).

In her statement, S.2593 co-sponsor and Senate Rules Committee Ranking Member Amy Klobuchar (D-MN) stated that "[a]ny changes that were recently made to the bill were made to accommodate the Republican leadership, and while some of us would have preferred the bill in its original form, we were ready to vote for the Chairman's mark." She contended that

> The bill contains important provisions for protecting our election infrastructure and would (1) require backup paper ballots for all states — including the nine that have partial paper ballots and the five that do not have them at all— in order to receive federal election funding; (2) require that all fifty states conduct post-election audits; and (3) require homeland security to immediately notify states of election infrastructure breaches.

In a statement to *Yahoo!*, White House spokesperson Lindsey Walters asserted that DHS "has all the statutory authority it needs to assist state and local officials to improve the security of existing election infrastructure." She added that "[w]e cannot support legislation with inappropriate mandates or that moves power or funding from the states to Washington for the planning and operation of elections."

Other Hearings

"Accountability and Oversight of the Federal Communications Commission" – House Energy and Commerce/Communications and Technology

Further Reading

"Forget The Trade War. TikTok Is China's Most Important Export Right Now." – *BuzzFeed News*
"Huawei will commit to 'no-spy agreements' to win government contracts, chairman says amid US pressure on allies over 5G fears" – *South China Morning Post*
"Welcome to TrumpTok, a Safe Space From Safe Spaces" – *The New York Times*
"Russian government hackers targeted small county in Florida panhandle in 2016" – *The Washington Post*
"Documents reveal DOE struggles in hacking whodunits" – *E&E News*
"Facebook busts Israel-based campaign to disrupt elections" – *AP News*
"The Trade Secret: Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers" – *ProPublica*
"Lawmakers seek probe on U.S. hacking services sold globally" – *Reuters*
"Identity crisis: FBI plays catch-up as cyberthreats escalate" – *Yahoo! News*
"Iran's coming response: Increased terrorism and cyber attacks?" – *The Hill*
"NSO owner tells Amnesty it will prevent abuse of spyware linked to WhatsApp breach" – *Reuters*
"Macron, Ardern lead call to eliminate online terrorist content" – *Politico Europe*
"Report: Iran-linked disinformation effort had personal touch" – *AP News*
"No sign that Beijing will offer a no-spy deal: Germany" – *Reuters*
"Apple chargers are getting hit by Trump's trade war" – *The Verge*