Technology Policy Update
22 March 2020
By Michael Kans, Esq.

FISA Authorities Lapse; Reauthorization Stalls

Last week, the Senate started the process of invoking cloture on H.R.6172 before leaving for the weekend, and these authorities lapsed on March 15 when the current authorization ended. The Senate is scheduled to hold a vote to invoke cloture on the motion to proceed to the bill at 5:30 pm. During floor consideration on March 12, Senator Mike Lee (R-UT) twice asked for unanimous consent to pass a clean 45-day extension of the expiring FISA authorities and then the consideration of amendments to H.R. 6172 offered by Members looking to reform and limit FISA, but Senate Intelligence Committee Chair Richard Burr (R-NC) objected to each request.

The week before, the House passed the "USA FREEDOM Reauthorization Act of 2020" (H.R. 6172) by a 278-136 vote, a bill to reauthorize three expiring Foreign Intelligence Surveillance Act (FISA) provisions used by the National Security Agency (NSA) primarily to conduct surveillance: the business records exception, roving wiretaps, and the "lone wolf" provision. However, the Senate declined to act immediately on the bill and opted instead to send a 77-day extension of these now lapsed authorities to the House, which is currently in recess.

A few weeks ago, the House Judiciary Committee set a February 26 markup of the bill that had been agreed upon with the House Intelligence Committee. However, Representative Zoe Lofgren (D-CA), was dissatisfied with the bill, calling it "so pitiful that it is not even worth pursuing." She added that "[w]e have the opportunity to reform the system…[and] [w]e should take that opportunity." Reportedly, Lofgren was going to offer amendments changing the bill to require that an amici curiae be appointed to oppose every government application under FISA to surveil an American and to change the definition of business records to exclude cell phone location, web browsing data, and search history. Information on the other amendments was not made available.

H.R. 6172 would end the controversial Call Detail Record (CDR) program that replaced the bulk telephony metadata program exposed by former NSA contractor Edward Snowden. The NSA had already shut down this program over what it framed as technical issues and deleted all the CDRs acquired from telecommunications companies, and yet, the Trump Administration asked that the program be reauthorized and vowed not to restart it until a need arose for these authorities. However, this request was coolly received by many Republicans and Democrats.

Also, H.R. 6172 would reauthorize the business records exception, which includes "any tangible thing," in FISA first instituted in the USA PATRIOT Act in 2001 but would reform certain aspects of the program. For example, if the Federal Bureau of Investigation (FBI) or NSA is seeking a business record under FISA for which a law enforcement agency would need to obtain a warrant, then the FBI or NSA will also need to obtain a warrant. Currently, this is not the case. Additionally, under H.R.6172, the FISA application process under Section 215 could not be used to obtain a person's cell site location or GPS information. However, the FBI or NSA would still be able to use Title I of FISA to seek cell site location or GPS data for purposes of conducting electronic surveillance related to alleged foreign intelligence. The bill would require that prosecutors must

inform defendants of the evidence derived from electronic surveillance unless doing so would harm national security.

Moreover, records obtained under Section 215 could be retained no longer than five years subject to a number of exceptions that may serve to make this limitation a dead letter. For example, if such records are deemed to have a "secret meaning" or are certified by the FBI as being vital to national security, then such records may be held longer than five years. Given the tendency of agencies to read their authority as broadly as possible and the past record of IC agencies, it is likely these authorities will be stretched as far as legally possible. It bears note that all restrictions are prospective, meaning that current, ongoing uses of Section 215 would be exempted. The business records provision would be extended until December 1, 2023 as are the other two expiring authorities that permit so-called roving wiretaps and allow for surveillance of so-called "lone wolves."

For FISA applications under Title I (i.e. electronic surveillance), any agency seeking a FISA order to surveil will need to disclose to the FISA court any information that may call into question the accuracy of the application or any doubtful information. Moreover, certain FISA applications to surveil Americans or residents would need to spell out the proposed investigative techniques to the FISA court. Moreover, any FISA application targeting U.S. officials or candidates for federal office must be approved by the Attorney General in writing before they can be submitted. H.R.6172 would permit the suspension or removal of any federal official, employee, or contractor for misconduct before the FISA court and increases criminal liability for violating FISA from five to eight years. Most of these reforms seem aimed at those Members, many of whom are Republican, that were alarmed by the defects in the FISA surveillance process of Trump Campaign associate Cater Page as turned up by the Department of Justice's Office of the Inspector General investigation. Some of these Members were opposed to the House Judiciary Committee's initial bill, which they thought did not implement sufficient reforms to the larger FISA process.

Like the bill the House Judiciary Committee was to mark up, the "USA FREEDOM Reauthorization Act of 2020" would set a six-month deadline for the Director of National Intelligence to declassify significant FISA opinions, orders, and decisions. The bill also beefs up the adversarial procedures in the FISA process by expanding the process by which amici curiae are expanded and their ability to ability FISA decisions to the FISA review court would also be expanded. Additionally, both FISA courts and the FISA review court would be empowered to seek outside legal counsel.
The Intelligence Committees would see their power increased to seek and obtain FISA applications in order to conduct oversight of the FISA process.

Finally, the powers of the Privacy and Civil Liberties Oversight Board (PCLOB) to oversee the FISA process would also be expanded. PCLOB would need to report on the extent to which FISA investigations are arising from protected First Amendment activities and from protected characteristics such as race, gender, sexual orientation, and others. There are broader PCLOB reforms that, for example, lengthen PCLOB members' terms to six years and allows them to serve past the six-year mark until a successor is confirmed by the Senate as is the case with many other agencies.

During floor debate on H.R. 6172, House Judiciary Committee Chair Jerrod Nadler (D-NY) explained "[i]t is by no means a perfect bill…[and] [t]here are many other changes to FISA that I would have liked to have seen here, but this bill includes very important reforms:

- First and foremost, it ends the NSA's Call Detail Records program, which began as part of a secret and unlawful surveillance project almost 20 years ago.
- This bill also prohibits the use of Section 215 to acquire information that would otherwise require a warrant in the law enforcement context. Our understanding of the Fourth Amendment has come to recognize a privacy interest in our physical location, and this legislation provides new protections accordingly.
- As the law continues to evolve, the public will see how the government applies these standards in the FISA court. This bill requires the government to disclose all significant opinions of the FISA court within 180 days.
- The bill also requires a one-time historical review of all significant opinions issued by the court since its inception.

Nadler stated the bill was changed to address the concerns of stakeholders on the left and right:

- To address the concerns of those who seek additional guarantees of privacy, we have added new retention limits, new reports to explain key legal issues, and an explicit prohibition on the use of Section 215 to obtain GPS and cell site location information.
- Other Members asked us to address the deep structural flaws in FISA identified by the inspector general in the report issued late last year. We have done just that. Working with our Republican colleagues, we have mandated additional transparency in FISA applications, created additional scrutiny for cases that involve elected officials, and elevated the consequences for misrepresenting information to the FISA court.

Lofgren argued against passage of the bill:

- I would like to quote from the American Civil Liberties Union letter received today. The American Civil Liberties Union strongly urges us to vote "no" on this bill. They say: "Over the last several years, it has been abundantly clear that many of our surveillance laws are broken."
- But that, "disappointingly, the reforms contained in H.R. 6172 are minimal—in many cases merely rep-resenting a codification of the status quo. In addition," the ACLU says, "the bill contains provisions that would be a step back from even our flawed current law."
- The ACLU goes on to say that "the bill fails to require that individuals receive appropriate notice and access to information when FISA information is used against them," that "the bill fails to fully address deficiencies with the FISA court that have led to illegal surveillance," that "the bill fails to appropriately limit the types of information that can be collected under Section 215," that "the bill fails to appropriately raise the standard for collecting information under Section 215," and that "the bill fails to appropriately limit the retention of information collected under Section 215.'

Congressionally Created Panel Releases Cyberspace Recommendations and Legislative Proposals

The Cyberspace Solarium Commission (CSC) released its final report and made a range of recommendations, some of which were paired with legislative language the CSC has not yet made available. The CSC was created by the National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232) to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI) served as co-chairs for the CSC, which also

included Representative James Langevin (D-RI), Senator Ben Sasse (R-NE), the Federal Bureau of Investigation Director Christopher Wray, Deputy Secretary of Defense David L. Norquist, and others.

The co-chairs explained

> We didn't solve everything in this report. We didn't even agree on everything. There are areas, such as balancing maximum encryption versus mandatory lawful access to devices, where the best we could do was provide a common statement of principles. Yet every single Commissioner was willing to make compromises in the course of our work because we were all united by the recognition that the status quo is not getting the job done. The status quo is inviting attacks on America every second of every day. The status quo is a slow surrender of American power and responsibility. We all want that to stop. So please do us, and your fellow Americans, a favor. Read this report and then demand that your government and the private sector act with **speed and agility** to secure our cyber future.

Nonetheless, they offered some "big ideas to get the conversation started:

- First, **deterrence is possible in cyberspace**. Today most cyber actors feel undeterred, if not emboldened, to target our personal data and public infrastructure. In other words, through our inability or unwillingness to identify and punish our cyber adversaries, we are signaling that interfering in American elections or stealing billions in U.S. intellectual property is acceptable. e federal government and the private sector must defend themselves and strike back with **speed and agility**. This is difficult because the government is not optimized to be quick or agile, but we simply must be faster than our adversaries in order to prevent them from destroying our networks and, by extension, our way of life. Our strategy of *layered cyber deterrence* is designed with this goal in mind. It combines enhanced resilience with enhanced attribution capabilities and a clearer signaling strategy with collective action by our partners and allies. It is a simple framework laying out how we evolve into a hard target, a good ally, and a bad enemy.
- Second, **deterrence relies on a resilient economy**. During the Cold War, our best minds were tasked with developing Continuity of Government plans to ensure that the government could survive and the nation recover after a nuclear strike. We need similar planning today to ensure that we can reconstitute in the aftermath of a national-level cyberattack. We also need to ensure that our economy continues to run. We recommend that the government institute a Continuity of the Economy plan to ensure that we can rapidly restore critical functions across corporations and industry sectors, and get the economy back up and running after a catastrophic cyberattack. Such a plan is a fundamental pillar of deterrence—a way to tell our adversaries that we, as a society, will survive to defeat them with **speed and agility** if they launch a major cyberattack against us.
- Third, **deterrence requires government reform.** We need to elevate and empower existing cyber agencies, particularly the Cybersecurity and Infrastructure Security Agency (CISA), and create new focal points for coordinating cybersecurity in the executive branch and Congress. To that end, we recommend the creation of a National Cyber Director with oversight from new congressional Cybersecurity Committees, but our goal is not to create more bureaucracy with new and duplicative roles and organizations. Rather, we propose giving existing organizations the tools they need to act with **speed and agility** to defend our networks and impose costs on our adversaries. The key is CISA, which we have tried to empower as the lead agency for federal cybersecurity and the private sector's preferred

partner. We want working at CISA to become so appealing to young professionals interested in national service that it competes with the NSA, the FBI, Google, and Facebook for top- level talent (and wins).

- Fourth, **deterrence will require private-sector entities to step up and strengthen their security posture.** Most of our critical infrastructure is owned by the private sector. at is why we make certain recommendations, such as establishing a cloud security certification or modernizing corporate accountability reporting requirements. We do not want to saddle the private sector with onerous and counterproductive regulations, nor do we want to force companies to hand over their data to the federal government. We are not the Chinese Communist Party, and indeed our best path to beating our adversaries is to stay free and innovative. But we need C-suite executives to take cyber seriously since they are on the front lines. With support from the federal government, private-sector entities must be able to act with **speed and agility** to stop cyberattackers from breaking out in their networks and the larger array of networks on which the nation relies.
- Fifth, **election security must become a priority**. The American people still do not have the assurance that our election systems are secure from foreign manipulation. If we don't get election security right, deterrence will fail and future generations will look back with longing and regret on the once powerful American Republic and wonder how we screwed the whole thing up. We believe we need to continue appropriations to fund election infrastructure modernization at the state and local levels. At the same time, states and localities need to pay their fair share to secure elections, and they can draw on useful resources—such as nonprofits that can act with greater **speed and agility** across all 50 states—to secure elections from the bottom up rather than waiting for top-down direction and funding. We also need to ensure that regardless of the method of casting a vote, paper or electronic, a paper audit trail exists (and yes, we recognize the irony of a cyber commission recommending a paper trail).

The CSC stated

> We didn't solve everything in this report. We didn't even agree on everything. There are areas, such as balancing maximum encryption versus mandatory lawful access to devices, where the best we could do was provide a common statement of principles. Yet every single Commissioner was willing to make compromises in the course of our work because we were all united by the recognition that the status quo is not getting the job done. The status quo is inviting attacks on America every second of every day. The status quo is a slow surrender of American power and responsibility. We all want that to stop. So please do us, and your fellow Americans, a favor. Read this report and then demand that your government and the private sector act with **speed and agility** to secure our cyber future.

The CSC stated that "[a]fter conducting an extensive study including over 300 interviews, a competitive strategy event modeled after the original Project Solarium in the Eisenhower administration, and stress tests by external red teams, the Commission advocates a new strategic approach to cybersecurity: layered cyber deterrence." The CSC explained that "[t]he desired end state of layered cyber deterrence is a reduced probability and impact of cyberattacks of significant consequence...[and] [t]he strategy outlines three ways to achieve this end state:

> 1. Shape behavior. The United States must work with allies and partners to promote responsible behavior in cyberspace.
> 2. Deny benefits. The United States must deny benefits to adversaries who have long exploited cyberspace to their advantage, to American disadvantage, and at little cost to

themselves. This new approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem.

3. Impose costs. The United States must maintain the capability, capacity, and credibility needed to retaliate against actors who target America in and through cyberspace."

The CSC made a host of recommendations generally but also linked some of the recommendations to legislative proposals drafted by CSC staff. However, these drafts have not yet been released even though the CSC claims "[l]egislative proposals are available online at www.solarium.gov. Nonetheless, the CSC made clear it does not necessarily support these proposals:

- PILLAR 1: REFORM THE U.S. GOVERNMENT'S STRUCTURE AND ORGANIZATION FOR CYBERSPACE
  - Recommendation 1.2: Create House Permanent Select and Senate Select Committees on Cybersecurity
  - Recommendation 1.3: Establish a National Cyber Director
  - Recommendation 1.4.1: Codify and Strengthen the Cyber Threat Intelligence Integration Center
  - Recommendation 1.5: Diversify and Strengthen the Federal Cyberspace Workforce
- PILLAR 2: STRENGTHEN NORMS AND NON-MILITARY INSTRUMENTS OF POWER
  - Recommendation 2.1: Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State
  - Recommendation 2.1.4: Improve International Tools for Law Enforcement Activities in Cyberspace [Provide MLAT Subpoena Authority and Increase FBI Cyber ALATs]
  - Recommendation 2.1.5: Leverage Sanctions and Trade Enforcement Actions [Codify Executive Order 13848]
- PILLAR 3: PROMOTE NATIONAL RESILIENCE
  - Recommendation 3.1: Codify Sector-specific Agencies into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk
  - Recommendation 3.1.1: Establish a Five-Year National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy
  - Recommendation 3.1.2: Establish a National Cybersecurity Assistance Fund to Ensure Consistent and Timely Funding for Initiatives at Underpin National Resilience
  - Recommendation 3.2: Develop and Maintain Continuity of the Economy Planning
  - Recommendation 3.3: Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund"
  - Recommendation 3.3.2: Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts
  - Recommendation 3.3.5: Establish a Biennial National Cyber Tabletop Exercise
  - Recommendation 3.3.6: Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard
  - Recommendation 3.4: Improve the Structure and Enhance Funding of the Election Assistance Commission
  - Recommendation 3.4.1: Modernize Campaign Regulations to Promote Cybersecurity

- Recommendation 3.5: Build Societal Resilience to Cyber-Enabled Information Operations [Educational and Awareness Grant Programs]
- Recommendation 3.5.1: Reform Online Political Advertising to Defend against Foreign Influence in Elections

- PILLAR 4: RESHAPE THE CYBER ECOSYSTEM TOWARD GREATER SECURITY
  - Recommendation 4.1: Establish and Fund a National Cybersecurity Certification and Labeling Authority
  - Recommendation 4.1.1: Create or Designate Critical Technology Security Centers
  - Recommendation 4.2: Establish Liability for Final Goods Assemblers
  - Recommendation 4.3: Establish a Bureau of Cyber Statistics
  - Recommendation 4.4: Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications
  - Recommendation 4.4.4: Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements
  - Recommendation 4.5: Develop a Cloud Security Certification
  - Recommendation 4.5.1: Incentivize the Uptake of Secure Cloud Services for Small and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments
  - Recommendation 4.5.2: Develop a Strategy to Secure Foundational Internet Protocols and Email
  - Recommendation 4.5.3: Strengthen the U.S. Government's Ability to Take Down Botnets
  - Recommendation 4.6: Develop and Implement an Information and Communications Technology Industrial Base Strategy
  - Recommendation 4.7: Pass a National Data Security and Privacy Protection Law
  - Recommendation 4.7.1: Pass a National Breach Notification Law
- PILLAR 5: OPERATIONALIZE CYBERSECURITY COLLABORATION WITH THE PRIVATE SECTOR
  - Recommendation 5.1: Codify the Concept of "Systemically Important Critical Infrastructure"
  - Recommendation 5.1.1: Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector
  - Recommendation 5.1.2: Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities
  - Recommendation 5.1.3: Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities
  - Recommendation 5.2: Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information
  - Recommendation 5.2.2: Pass a National Cyber Incident Reporting Law
  - Recommendation 5.2.3: Amend the Pen Register Trap and Trace Statute to Enable Better Identification of Malicious Actors
  - Recommendation 5.3: Strengthen an Integrated Cyber Center within CISA and Promote the Integration of Federal Cyber Centers
  - Recommendation 5.4.1: Institutionalize Department of Defense Participation in Public-Private Cybersecurity Initiatives
- PILLAR 6: PRESERVE AND EMPLOY THE MILITARY INSTRUMENTS OF POWER

- Recommendations 6.1 & 6.1.3: Direct the Department of Defense to Conduct a Force Structure Assessment of the Cyber Mission Force / Review the Delegation of Authorities for Cyber Operations
- Recommendation 6.1.1: Direct the Department of Defense to Create a Major Force Program Funding Category for U.S. Cyber Command
- Recommendation 6.1.7: Assess the Establishment of a Military Cyber Reserve
- Recommendation 6.2: Conduct a Cybersecurity Vulnerability Assessment of All Segments of the NC3 and NLCC Systems and Continually Assess Weapon Systems Cyber Vulnerabilities
- Recommendation 6.2.1: Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program
- Recommendation 6.2.2: Require Threat Hunting on Defense Industrial Base Networks
- Recommendation 6.2.4: Assess and Address the Risk to National Security Systems Posed by Quantum Computing

It is unlikely that Congress will adopt most of these recommendations by turning them into statute, but the Administration will likely pick and choose those it will implement without obtaining new or further authority. However, these recommendations will serve to inform the debate on cyber-related issues going forward.

HASC Hearing on Administration's FY 2021 Budget Request For Cyber Command

The House Armed Services Committee's Intelligence and Emerging Threats and Capabilities Subcommittee heard testimony on the Trump Administration's FY 2021 budget request for U.S. Cyber Command and cyberspace operations. Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor to the Secretary of Defense Kenneth Rapuano and U.S. Cyber Command head and National Security Agency Director General Paul Nakasone appeared before the subcommittee.

Chair Jim Langevin (D-RI) noted that "[t]he Department of Defense created U.S. Cyber Command (CYBERCOM) in 2009, and more than ten years later, we are still working diligently on establishing the foundations, concepts, doctrine, training, and metrics needed to ensure the security of the nation in the cyberspace domain." He claimed that "[t]he state of cyber in national defense is more central than ever, and 2020 marks a sea change, with cyber firmly established and accepted as a warfighting domain, capability, and asset…[and] [t]his is highlighted best through the current operational posture and institutional maturation of CYBERCOM." Langevin stated that "[o]ver the course of 2020, this subcommittee expects the Command to aggressively address issues of readiness, operational tempo, and the defense of the nation's electoral system."

Langevin stated that "[t]his Committee has worked to ensure that the Department, the military services, and CYBERCOM are equipped with the tools and authorities necessary to achieve their objectives…[and] [i]n the FY 2020 [National Defense Authorization Act] (NDAA) (P.L. 116-92), we granted new authorities to CYBERCOM, and bolstered multiple frameworks for legislative oversight." He stated that "[w]e seek to balance an appropriate degree of oversight while ensuring the command retains operational flexibility. We will continue this trend through our collective work in the FY 2021 [NDAA]."

Langevin stated that "CYBERCOM is facing possibly the most challenging year in its existence… [and] General Nakasone, your command sits at the center of the Department's efforts to secure the information environment." He claimed that "[t]he United States faces increasing malicious cyberactivity from Russia, Iran, China, and others." Langevin said that "[w]e know about how Russia weaponized information during the 2016 election, and we must do more to anticipate and counter these sophisticated operations." He claimed that "[w]hile we have had some success countering Russia's malign influence campaigns in 2018, we must not let our guard down…[and] [w]e must ensure that we are properly organized within the Department of Defense and coordinating across the U.S. Government."

Langevin stated that "[f]or the past year, I have had the privilege of serving on the Cyberspace Solarium Commission – and I thank you, Mr. Rapuano, for your many contributions to our work… [and] [o]ne of the areas of focus of the commission has been whether CYBERCOM's force structure properly reflects the Command's operational aspirations." He added that "[e]ssentially, we need to candidly assess whether a force conceived more than seven years ago is sufficient for a dramatically different environment today… [and] I will also be curious to hear candid assessments on how organic capabilities resident in the Services are rationalized with CYBERCOM's mission and strategy."

Langevin stated that "[w]hile I fully support CYBERCOM's more offensively postured construct, I am concerned that the President's FY 2021 cyber budget signals in select places that we can sacrifice defensive programs and investments in favor of investments in offensive cyber systems and programs."

Ranking Member Elise Stefanik (R-NY) stated that it has been two years since US CYBERCOM reach full operational capacity, and in that time there have been several significant achievements with tangible operational results. She stated these included the inter-agency efforts with the Russia small group and Operation Synthetic Theology and the development and implementation of a strategy that emphasizes continuous engagement, hunting adversaries forward, and reasserting deterrence in cyberspace. Stefanik claimed that during this time, the U.S.'s adversaries have adapted by blending cyber and information warfare to form an operational continuum that continues to challenge the U.S. in the digital realm. She asserted that what worked for U.S. cyber forces in helping to secure the 2018 mid-term elections will not necessarily guarantee U.S. safety moving forward. Stefanik counseled that the U.S. must acknowledge the creativity of its adversaries and continue to adapt the U.S.'s playbook. Stefanik added that the U.S. must ensure that election security is a continuous sustained effort.

Stefanik claimed there has been significant progress within the cyber mission workforce over the last year, specifically the understanding and categorizing of specific cyber operations forces, the delegation of important operational authorities, the establishment of cyber-peculiar ability, and the understanding of cyber vulnerability within U.S. installations and weapons systems. Stefanik said the U.S. has made headway to mature cyber forces but much work lies ahead. She stated she wanted to hear what has been learned about the needs of the cyber operational force to meet the future needs of the U.S. Stefanik asserted that as the U.S. reevaluates its cyber posture such information will be critical to ensure the appropriate resources are aligned with policies and authorities in order for the U.S. to stay ahead of its adversaries and reaffirm the notion of deterrence in cyberspace.

Rapuano stated that "I would like to offer our perspective on the current threat environment… [and] [a]s our National Defense Strategy (NDS) makes clear, we are in a renewed era of great power competition." Rapuano said that "[s]trategic competitors such as Russia and China are asserting their military and non-military power to challenge the rules- based international order… [and] [a]lthough our military superiority has deterred conventional aggression against the United States, states such as China, Russia, North Korea, and Iran are increasingly taking actions in the gray zone below the threshold of the use of force to undermine our security." He contended that "[t]here is perhaps no area where this is more true than in cyberspace."

Rapuano stated

- It is in this context of determined, rapidly maturing adversaries that the 2018 DOD Cyber Strategy called for a more proactive approach to competing in the domain. We can no longer allow our strategic competitors to flout norms of responsible state behavior in cyberspace while claiming to be responsible actors. The DOD Cyber Strategy normalizes the Department's activities in cyberspace by directing the Joint Force to integrate cyber operations fully into military operations. The Cyber Strategy also makes clear that the Department's focus in cyberspace, like in other domains, is to prevent or mitigate threats before they harm U.S. national interests. The Department will "defend forward" in cyberspace in the same way we operate outside our borders on land, in the air, at sea, and in space to understand and defeat threats before they reach the United States.
- The Department defends forward by conducting operations that range from collecting information about hostile cyber actors, to exposing malicious cyber activities and associated infrastructure publicly, to directly disrupting malicious cyber actors. In order to be successful, we must be in malicious cyber actors' networks and systems and continually refresh our accesses, capabilities, and intelligence. Defending forward simultaneously puts "sand in the gears" of the offensive operations of malicious cyber actors, and generates the insights that enable our interagency, industry, and international partners to strengthen their resilience, address vulnerabilities, and defend critical networks and systems.

Nakasone stated

> Today, we are 244 days from the 2020 Presidential election. Last year, we institutionalized our efforts from the Russia Small Group before the 2018 elections into an enduring Election Security Group for 2020 and beyond. The group reports directly to me and is led by representatives from Cyber Command and the National Security Agency. Its objectives are to generate insights that lead to improved defenses and being prepared, if ordered, to impose costs on those who seek to interfere. To be sure, we place a high priority on collecting and sharing information with our partners at DHS and FBI to enable their efforts as part of a whole- of-government approach to election security. But Cyber Command's authorities mean that it must also be prepared to act.

Nakasone asserted that

In 2018, these actions helped disrupt plans to undermine our elections. During multiple hunt forward missions, Cyber Command personnel were invited by other nations to look for adversary malware and other indicators of compromise on their networks. Our personnel not only used that information to generate insights about the tradecraft of our adversaries, but also to enable the defenses of both our foreign and domestic partners. And by disclosing that information publicly to

private-sector cybersecurity providers, they took proactive defensive action that degraded the effectiveness of adversary malware.

Nakasone stated

- Cyber Command also executed offensive cyber and information operations. Each featured thorough planning and risk assessments of escalation and other equities. Each was coordinated across the interagency. And each was skillfully executed by our professional forces. Collectively, they imposed costs by disrupting those planning to undermine the integrity of the 2018 midterm elections.
- Cyber Command's contributions to broader government efforts to protect elections are part of its mission to defend the nation in cyberspace. To defend the nation from this and other kinds of malicious cyber activity, persistent engagement with our adversaries allows Cyber Command to generate new insights that drive new methods of defense, and inform future options to impose cost. This approach drives the Election Security Group's approach to the 2020 elections, ensuring that exquisite intelligence drives tailored operations, which in turn generate more insight and opportunities to harden defenses and impose costs if necessary.

DHS FY 2021 Budget Request Hearing

The House Homeland Security Committee's Cybersecurity, Infrastructure Protection, & Innovation Subcommittee examined the FY 2021 budget requests of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and Science and Technology Directorate (S&T).

Subcommittee Chair Cedric Richmond (D-LA) stated I will be interested in know if the FY 2021 budget request for CISA is sufficient to implement the recommendations aimed at increasing CISA's capacity and, if not, what additional resources will be necessary. He stated that at the outset, I want to debunk the myth that Federal agencies can do more with less., and I support eliminating waste and increasing efficiency, but the fact is that with more you can do more. Richmond asserted that technology is evolving and creating opportunities for our adversaries to hack critical infrastructure, disrupt our elections, and hold State and local government networks hostage. He claimed that CISA must be equipped to be an effective Federal partner and S&T must be positioned to develop and identify technology to strengthen our defenses. He argued the President's FY 2021 budget does fails both of these important components.

Richmond remarked that last year, Committee Democrats led a bipartisan letter to appropriators seeking additional funding for CISA's cybersecurity mission, and we succeeded in increasing CISA's cyber budget by $350 million, accelerating efforts to secure Federal networks and ramping up CISA's threat analysis and response capabilities for private sector critical infrastructure owners and operators and State and local governments. He added that despite bipartisan support for increasing CISA's cybersecurity budget, the President's Budget cuts it by about over $150 million. Richmond stated I do not understand how a cut of that magnitude makes communities trying to defend themselves against ransomware attacks, Federal networks, or critical lifeline services – from power to communications – any more secure.

Richmond stated that I am also concerned about the Administration's continued efforts to cut S&T, and despite ample evidence that U.S. investment in research and development is lacking, this budget cuts research and development (R&D) for cybersecurity as well as important University

Programs and Centers of Excellence. He said that we cannot afford to continue to defer investments in R&D, and I will work hard to restore funding.

Ranking Member John Katko (R-NY) stated that our nation faces digital and physical threats daily that have the potential to disrupt, damage and destroy their targets, and these threats will only grow in magnitude, frequency, and sophistication in the years ahead as cyber adversaries particularly nation state actors seek political, economic, and national security advantages. He remarked that the federal government works with public and private sector partners to prevent and deter current threats, but also to plan for the future. Katko said that CISA was tasked by Congress in 2018 to serve as the nation's risk advisor, providing for the timely sharing of information, analysis and assessment, and facilitating resilience building and mitigation in the .gov domain, state and local governments, and the private sector across industries. He noted that during the past year CISA completed its transition to a stand-alone agency subject to DHS oversight, and I am interested in hearing how strengthening CISA's authorities could further clarify civilian cybersecurity risk management authorities and CISA's role as a convener of public-private partnerships. Katko stated that I look forward to hearing about CISA's plans to continue its progress securing our supply chain and tackling risks to our national critical functions and election infrastructure, and I invite Director Krebs to share his insights on CISA's work with state and local governments to secure 2020 elections from the hindsight of Super Tuesday and other election primaries.

Katko stated that today we also will hear from the Science & Technology Directorate, or S&T, about how they plan to execute their mission in the year ahead. He said that S&T, through partnerships within the federal government, academia and industry, develops innovative solutions to aid the Department of Homeland Security in achieving its mission more effectively, efficiently and affordably. Katko concluded by saying I look forward to hearing from both our witnesses and my colleagues to see how we can work together to ensure DHS is capable of protecting our nation from digital and physical threats.

CISA Director Christopher Krebs touched on highlights of the FY 2021 budget request:

- The FY2021 President's Budget includes $1.1 billion for cybersecurity initiatives at CISA to detect, analyze, mitigate, and respond to cybersecurity threats. We share cybersecurity risk mitigation information with government and non- government partners. By issuing guidance or directives to federal agencies, providing tools and services to all partners, and leading or assisting the implementation of cross-government cybersecurity initiatives, we are protecting government and critical infrastructure networks.
- Within the cybersecurity initiatives funding amount, the FY 2021 President's Budget includes $660 million for cybersecurity technology and services, including Continuous Diagnostics and Mitigation (CDM) and National Cybersecurity Protection System (NCPS) programs. These programs provide the technological foundation to secure and defend the Federal Government's information technology against advanced cyber threats.
- Funding for cybersecurity initiatives also includes $408 million for cybersecurity operations. Within this category, approximately $264 million is dedicated to threat hunting and vulnerability management operations. Threat hunting activity identify, analyze, and address significant cyber threats across all domains through detection activities, countermeasures development, as well as hunt and incident response services. Vulnerability management capabilities include assessments and technical services, such as vulnerability scanning and testing, penetration testing, phishing assessments, and red teaming on operational technology that includes the industrial control systems which

operate our Nation's critical infrastructure, as well as recommended remediation and mitigation techniques that improve the cybersecurity posture of our Nation's critical infrastructure.

- The FY 2021 President's Budget includes $158 million for emergency communications to ensure real-time information sharing among first responders during all threats and hazards. CISA enhances public safety interoperable communications at all levels of government across the country through training, coordination, tools, and guidance.
- The President's Budget includes $167 for the Integrated Operations Division. This division is charged with coordinating CISA's frontline, externally-facing activities in order to provide seamless support and an expedited response to critical needs. These funds include $82 million to support 373 protective security advisors and cybersecurity advisors located across the country. Protective Security Advisors conduct proactive engagement and outreach with government at all levels and critical infrastructure.
- The FY 2021 President's Budget fully funds CISA's risk management activities, including $91.5 million for the National Risk Management Center (NRMC). The NRMC is a planning, analysis, and collaboration center working to identify and address the most significant risks to our Nation's critical infrastructure. The NRMC also houses the National Infrastructure Simulation and Analysis Center (NISAC), which provides homeland security decision-makers with timely, relevant, high-quality analysis of cyber and physical risks to critical infrastructure across all sectors during steady state and crisis action operations. Increased funding will support election security, securing 5G telecommunications, and supply chain risk analysis.
- The President's Budget asks for $24 million within the Science and Technology Directorate (S&T) to continue research and development efforts in support of CISA's cybersecurity mission. CISA and S&T have made tremendous strides in collaborating to advance joint priorities. In FY 2019, CISA and S&T awarded a project to create a 'pipeline' for low technology readiness level efforts to mature and transition into CISA. Workstreams in this pipeline are advancing threat- driven cyber analytics and development of a cyber risk framework. This project is an important first step in the larger plan for CISA and S&T to enhance analytics in conjunction with big data and machine learning. Subsequent efforts in FY2020 and beyond are planned to leverage hyperscale cloud platforms and significantly advance the data and analytics capabilities of CISA.

Acting Deputy Under Secretary of Homeland Security for Science and Technology Andre Hentz noted a request of $643.7 million for S&T within DHS for some of these programs:

- A strong cross-Department Cybersecurity R&D program is critical for DHS. The Cyber Security & Infrastructure Security Agency (CISA) and S&T have made tremendous strides in resetting the relationship, directing R&D resources into mission support of CISA requirements. CISA and S&T have established repeatable processes to identify capability gaps, prioritize needs, and execute on RD&I needs. The FY 2021 Cybersecurity R&D budget request is for $24 million and places all Cyber R&D funding with S&T.
- S&T is currently partnered with the National Institutes of Artificial Intelligence (AI) with the goal of mitigating risks to misuse of AI, identifying opportunities and applications of AI within the homeland security mission space, improving privacy protection, and developing new governance and policy frameworks for artificial intelligence and machine learning. S&T is working with its operational DHS Component partners to assess opportunities for leveraging Automated Machine Learning (AutoML) and related data preparation tools as a means of accelerating understanding and use of this technology within the DHS enterprise. In FY 2021, S&T will examine and characterize the state of artificial

intelligence research relative to future homeland security mission applications. Research activities will focus on the development of core capabilities that enable trustworthy artificial intelligence to improve core automation capabilities that are secure, private, and trusted for critical homeland security applications.

- The FY 2021 Budget request provides $14.4 million for S&T's Probabilistic Analysis for National Threats Hazards and Risks (PANTHR) program that aligns S&T's chemical and biological hazard awareness and characterization activities to provide timely accurate and defensible decision support tools and knowledge to stakeholders. PANTHR is currently supporting the Countering Weapons of Mass Destruction Office (CWMD) to address the ongoing Coronavirus outbreak by providing consolidated up-to-date information regarding the virus to DHS components. PANTHR is currently leveraging the capabilities of one of the DHS laboratories, the National Biodefense Analysis and Countermeasure Center (NBACC), which is addressing pertinent scientific questions and DHS operational concerns regarding Coronavirus surface stability and decontamination. PANTHR funding in FY 2021 would further support the expansion of these national capabilities to address current and emerging chemical and biological concerns. Additionally, the FY 2021 request would allow PANTHR to develop additional assessment capabilities to address growing infrastructure concerns, such as the bio-economy, and fill other critical technical hazard data gaps regarding WMD risks to the Homeland.
- S&T is requesting $35.9 million in the FY 2021 budget to directly address Customs and Border Protection (CBP), the U.S. Coast Guard (USCG), the U.S. Secret Service (USSS), and the Federal Protective Service (FPS) requirements for Countering Unmanned Aircraft System (CUAS) requirements. In close coordination with our operational customers, S&T is responsible for the initial CUAS deployment architecture, technology selection, system integration, system test, training and cyber compliance. The FY 2021 S&T CUAS investment will focus on mission interoperability with the Department of Defense and Department of Justice in the National Capital Region, improved CUAS capabilities for DHS components, and addressing future threats. UAS threats to critical infrastructure and security activities will likely increase in the near future as the number of UAS introduced into the national airspace continues to increase. However, currently the use of technical means to detect, track, and disrupt malicious UAS operations remains limited.
- S&T is dedicated to developing or adopting innovative tools for DHS Components, and the FY 2021 Budget request supports that effort. For example, the S&T Opioid Detection project continues to integrate advanced technologies, including narcotics anomaly detection algorithms and chemical sensing technologies, into CBP international mail facilities, and to evolve efforts directed at detecting synthetic opioids in additional operational environments in response to changing trafficking dynamics. Increased funding will also further improve the understanding of supply chain logistics and intelligence to aid in targeting, investigations, and ultimately, disruption of international smuggling. The administration is also focusing on Targeted Violence and Terrorism Prevention, and S&T is a vital partner using research to inform policy, strategy, tactics, techniques and procedures. S&T is actively working to support technology integration and techniques to reduce the likelihood of mass violence and improve the ability to prevent and respond to a mass violence event.

GAO Reports On Administration Efforts To Drive Adoption of Framework and Close Down Unneeded Data Centers

The Government Accountability Office (GAO) examined the extent to which the nine agencies with responsibility for the 16 critical infrastructure sectors have determined how widely critical infrastructure owners and operators have adopted the National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" (Framework). GAO issued this report under a statutory requirement to periodically determine how well the sector-specific agencies (SSA) are encouraging the private owners and operators of critical cyber infrastructure to adopt and implement the Framework. While the GAO found some improvement since its last assessment, many of the agencies still do not know how widely and the extent to which the Framework has been adopted. Conceivably, the committees of jurisdiction over NIST and cybersecurity could hold hearings and/or contemplate legislation to spur SSAs to more effectively drive use of the Framework.

The GAO noted

- Most of the SSAs have not determined the level and type of framework adoption, as we previously recommended. Most of the sectors, however, had efforts underway to encourage and facilitate use of the framework. Even with this progress, implementation of our recommendations is essential to the success of protection efforts.
- While selected organizations reported varying levels of improvements, the SSAs have not collected and reported sector-wide improvements as a result of framework use. The SSAs and organizations identified impediments to collecting and reporting sector-wide improvements, including the lack of precise measurements of improvement, voluntary nature of the framework, and lack of a centralized information sharing mechanism.
- However, NIST and [the Department of Homeland Security] (DHS) have initiatives to help address these impediments. These included an information security measurement program, cybersecurity framework starter profile, information sharing programs, self-assessment tools, and surveys to support SSAs in measuring and quantifying improvements in the protection of critical infrastructure as a result of using the framework.
- However, NIST has yet to establish time frames for completing the information security measurement program and starter profile. Moreover, the SSAs have yet to report on sector-wide improvements using the initiatives. Until they do so, the critical infrastructure sectors may not fully understand the value of the framework to better protect their critical infrastructures from cyber threats.

The GAO made "the following 10 recommendations to NIST and the nine sector-specific agencies:

- The Director of NIST should establish time frames for completing NIST's initiatives, to include the information security measurement program and the cybersecurity framework starter profile, to enable the identification of sector-wide improvements from using the framework in the protection of critical infrastructure from cyber threats. (Recommendation 1)
- The Secretary of Agriculture, in coordination with the Secretary of Health and Human Services, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 2)
- The Secretary of Defense should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 3)

- The Secretary of Energy should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 4) The Administrator of the Environmental Protection Agency should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 5)
- The Administrator of the General Services Administration, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s), such as the Coordinating Council and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 6)
- The Secretary of Health and Human Services, in coordination with the Secretary of Agriculture, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 7)
- The Secretary of Homeland Security should take steps to consult with respective sector partner(s), such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sectors using existing initiatives. (Recommendation 8)
- The Secretary of Transportation, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s) such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 9)
- The Secretary of the Treasury should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 10)

In another technology-related report, the GAO issued another of its periodic assessments of the Office of Management and Budget's (OMB) Data Center Optimization Initiative (DCOI), started in 2012 by the Obama Administration to shrink the federal government's footprint of data centers, increase efficiency and security, save money, and reduce energy usage. The DCOI was codified in the "Federal Information Technology Acquisition Reform" (FITARA) (P.L. 113-291) and extended in 2018 until October 1, 2020. The DCOI has gone through a number of iterations to change some of the program's focus, and most recently in June 2019, the Trump Administration issued a memorandum with the latest revisions.

The GAO found that 23 of the 24 agencies participating in the DCOI met or planned to meet their FY 2019 goals to close 286 of the 2,727 data centers considered part of the DCOI. This latter figure deserves some discussion, for the Trump Administration changed the definition of what is a data center to exclude smaller ones (so-called non-tiered data centers). GAO asserted that "recent OMB DCOI policy changes will reduce the number of data centers covered by the policy and both OMB and agencies may lose important visibility over the security risks posed by these facilities."

Nonetheless, these agencies are projecting savings of $241.5 million when all the 286 data centers planned for closure in FY 2019 actually close. It bears note that the GAO admitted in a footnote it "did not independently validate agencies' reported cost savings figures," so these numbers may not be reliable.

OMB's new memorandum also replaced the previous optimization metrics with revised measures that focused on (1) reporting the number of agencies' virtualized hosts, underutilized servers, and data centers with advanced energy metering; and (2) the percentage of time that data centers were expected to be available to provide services. In contrast to the previous DCOI guidance, the new memorandum did not specify government-wide performance targets for the optimization metrics, such as setting a target for server utilization of 65 percent for all agencies. Instead, OMB worked with agencies to establish agency-specific targets that were also identified in agency DCOI strategic plans and on the IT Dashboard. In addition, the guidance described how agencies could apply for an optimization performance exemption for data centers where typical optimization activities (consolidation of data collection, storage, and processing to a central location) were technically possible but increased the response time for systems beyond a reasonable limit.

Additionally, GAO judged how well the DCOI agencies met OMB's four new metrics:

- Virtualization: The number of servers and mainframes serving as virtual hosts in agency-managed data centers.
- Data center availability: Ratio of uptime to downtime in data centers.
- Advanced energy metering: The number of data centers with advanced energy metering covering the majority of their floor space.
- Server utilization: The number of underutilized production severs in federal data centers.

The GAO found that as "of September 2019:

- 11 reported that they had met their target for virtualization,
- 11 reported that they had met their advanced metering target, and
- 18 reported that they had met their server utilization target."

In a note to a chart, the GAO explained "[d]ue to variances in how agencies reported data for the data center availability metric, we determined that the data was not sufficiently reliable for us to report on agencies' progress for the availability metric."

In conclusion GAO stated

- Federal data center consolidation efforts have been underway since 2010, and agencies continue to report progress towards meeting their goals for data center closures and achieving related savings. Specifically, almost all of the 24 DCOI agencies met, or planned to meet, their goals for data center closures in fiscal year 2019. Additionally, in fiscal year 2019, almost all of the agencies met or planned to meet their $249 million total savings target. Agencies' efforts in both respects have made an important contribution to achieving the overall goals of DCOI. However, agencies' annual closure goals are not currently reported in their DCOI strategic plans or tracked on the IT Dashboard, requiring us to manually calculate those targets. Unless agencies' annual closure goals are fully reported and tracked, oversight of DCOI will be hampered. Further, the six agencies without plans to meet their fiscal year data center closure or cost savings targets will continue to be challenged to realize the full benefits of DCOI.

- As part of the 2019 changes to DCOI, OMB significantly reduced the scope of what is considered a data center, and, in doing so, excluded about 2,000 smaller facilities that were previously reported by agencies in 2018. While OMB previously acknowledged that these types of facilities inefficiently consume resources and pose security risks, agencies are no longer required to report these locations in their inventories. Further, there is currently no documentation of OMB's decisions on agency requests to remove data centers from reporting, or to exempt mission critical data centers from closure targets. By no longer reporting key facilities as part of DCOI and by not documenting decisions on which facilities are exempt from DCOI, oversight of agencies' consolidation and optimization efforts may be impaired, and agencies may remain exposed to the related vulnerabilities.
- Agencies' progress against OMB's three revised metrics was mixed, and, for one new metric, agencies reported data that varied so widely, we concluded the data for this metric were not sufficiently reliable for us to report on. However, in comparing OMB's four metrics against the characteristics of an effective metric, we most notably found that none of the metrics included appropriate performance parameters for evaluating agencies' progress against goals. Metrics that include more robust and informative agency performance data can play an important role in both achieving the optimization goals and mission of DCOI and allowing for stronger oversight of those efforts.

In terms of how to improve the DCOI, the GAO stated that "[i]n addition to reiterating our prior open recommendations to the agencies in our review regarding their need to meet DCOI's closure and savings goals and optimization metrics, we are making a total of eight new recommendations —four to OMB and four to three of the 24 agencies. Specifically:

- The Director of the Office of Management and Budget should (1) require that agencies explicitly document annual data center closure goals in their DCOI strategic plans and (2) track those goals on the IT Dashboard. (Recommendation 1)
- The Director of the Office of Management and Budget should require agencies to report in their quarterly inventory submissions those facilities previously reported as data centers, even if those facilities are not subject to the closure and optimization requirements of DCOI. (Recommendation 2)
- The Director of the Office of Management and Budget should document OMB's decisions on whether to approve individual data centers when designated by agencies as either a mission critical facility or as a facility not subject to DCOI. (Recommendation 3)
- The Director of the Office of Management and Budget should take action to address the key performance measurement characteristics missing from the DCOI optimization metrics, as identified in this report. (Recommendation 4)
- The Secretary of Agriculture should take action to achieve its data center- related cost savings target established under DCOI by OMB. (Recommendation 5)
- The Secretary of Commerce should take action to achieve its data center- related cost savings target established under DCOI by OMB. (Recommendation 6)
- The Secretary of Commerce should take action to meet its data center optimization metric targets established under DCOI by OMB. (Recommendation 7)
- The Administrator of the National Aeronautics and Space Administration should take action to achieve its data center-related cost savings target established under DCOI by OMB. (Recommendation 8)

Senate 5G Hearing

The Senate Commerce, Science, and Transportation Committee held its most recent hearing on 5G, titled "5G Supply Chain Security: Threats and Solutions." The hearing came at a time when two 5G-related bills were in the process of being sent to the White House: the "Secure and Trusted Communications Networks Act of 2019" (H.R.4998) and the "Secure 5G and Beyond Act of 2020" (S.893).

According to the Committee Report, H.R.4998 would:

- require the Federal Communications Commission (FCC or Commission) to develop and maintain a list of communications equipment and services that pose an unacceptable risk to national security and prohibit the use of Federal funds administered by the FCC to purchase, rent, lease, or otherwise obtain such equipment and services.
- establish[] the Secure and Trusted Communications Reimbursement Program to assist small communications providers with the costs of removing prohibited equipment and services from their networks and replacing prohibited equipment with more secure communications equipment and services.

S.893, according to its Committee Report, would:

- Require the President of the United States to develop a Federal Government-wide strategy to ensure the security of the Nation's next-generation—and future generations—wireless telecommunications systems and infrastructure.
- Direct the U.S. Government to assist allies and strategic partners in maximizing the security of next-generation wireless telecommunications systems, infrastructure, and software.

Chair Roger Wicker (R-MS) stated that closing the digital divide and positioning the United States to win the global race to 5G are priorities for this committee. He said that over the past several months, we have been discussing the wide-ranging economic and social benefits that broadband connectivity has delivered to communities across this country.

Wicker remarked that over the past few years, the United States Government, intelligence officials, and international allies have determined that telecommunications equipment from certain vendors, such as Huawei and ZTE, poses a national security risk. He stated that foreign adversaries and enemies of the United States have the capability of using this compromised equipment to spy on Americans, steal our intellectual property, or otherwise disrupt our way of life and economic well-being. Wicker said that to date, both Congress and the Trump Administration have taken a number of actions to address these security threats and protect our networks and devices from hostile exploitation. He contended that these actions include banning the use of Huawei and ZTE components in government systems; prohibiting the use of Universal Service Funds to purchase communications equipment and services from Huawei and ZTE, and other high-risk suppliers; and adding Huawei and its affiliates to the Entity List.

Wicker stated that most recently, Congress passed the "Secure and Trusted Communications Network Act" (H.R.4998), and when signed into law by President Trump in just a few days, this law establishes a critical "rip and replace" program for small and rural telecommunications operators to remove compromised equipment from their networks and replace it with components from trusted suppliers. He asserted that while this is a meaningful step forward in safeguarding the security of the nation's communications systems, the unfortunate reality is that our networks have already been compromised by foreign adversaries. Wicker claimed that we are seeing more reports that Huawei can covertly access mobile phone networks around the world, and at

the same time, some of our close allies are granting Huawei access to their communications systems.

Wicker said these are troubling developments, and we need to do more to shore up our own network defenses against hackers and state-sponsored actors, especially in our nation's rural and underserved communities. Wicker argued that this effort will require the development of a comprehensive strategy to secure the telecommunications supply chain. He noted that currently, Huawei maintains the largest global market share of telecommunications equipment, and the absence of a viable and affordable American or European alternative for end-to-end telecommunications components, including radios, chips, software, and devices, has enabled Huawei to increase its global influence.

Wicker said that at a time of rising global demand for 5G equipment, I hope witnesses will discuss what more Congress and the Administration can do to support trusted suppliers, invest in new technologies, and expand the domestic market for 5G network components. He stated that there are a number of international standards-setting organizations, such as the Third Generation Partnership Project or 3-G-P-P, and the International Telecommunications Union, that are developing technical standards for 5G. Wicker contended that U.S. participation in these organizations is also key to a secure telecommunications supply chain, and the hearing is an opportunity for witnesses to discuss how to increase U.S. engagement in the standards development process. He stated that this will help ensure American technical expertise and priorities are considered in the development of next-generation technologies. Wicker expressed his hope the committee will learn about how the telecommunications industry can improve its "cyber hygiene"- meaning what best practices companies could adopt to mitigate risks to vulnerable supply chains and will also learn about what more the Federal Communications Commission (FCC) can do to secure legacy networks and manage security risks in the transition to 5G.

Ranking Member Maria Cantwell (D-WA) said the committee has heard much about how 5G will advance the economy but none of this will happen unless these systems are secure. She remarked that a hearing the day before to review the Department of Energy's FY 2021 budget request, there was discussion about a cyber-attack that brought down a utility operating in the Western U.S. for 12 hours, meaning that concerns about this sort of hacking is no longer hypothetical. Cantwell stated that so far the discussion by policymakers about how to keep unsecure networks and equipment out of our domestic networks has been the focal point, but obviously eliminating the threat posed by these equipment is the highest priority. Cantwell added that the U.S. must raise its voice across the globe for no government backdoors. She asserted her belief that it is an imperative for the U.S. and its allies to foster a truly secure, diverse, and reliable supply chain for communications equipment. Cantwell contended we need to ensure that communications systems are secure and that the connections to those systems and software are also secure. Cantwell said in order to accomplish this, first and foremost, we need a broader strategic plan and acknowledged that recently passed "Secure 5G and Beyond Act of 2020" (S.893) directing the President to submit a much-needed strategy on 5G that will hopefully be developed and implemented soon.

Cantwell remarked that the U.S. must build a forceful global coalition of countries that share values and respect property rights and the rule of law. She added a smart multi-national approach is needed. Cantwell called for the committee to continue working with the Senate Foreign Relations and Intelligence Committees on this goal. She said that incentives must be

created for other countries to use equipment that does not contain government backdoor access, and the U.S. has great allies with which it can work on these issues.

Ericsson Network Product Solutions Head of Security Jason Boswell stated that we recommend that the Committee take the following steps:

> (1) Pass, implement, and oversee 5G security legislation. As I noted at the outset, the Senate's recent passage of Chairman Wicker's Secure and Trusted Communications Networks Act represents a thoughtful and crucial step forward. We look forward to the President signing this bill and stand ready to work with the small operators who will have to replace existing equipment. As the Committee is well aware, further opportunities to build on the momentum of that legislation await, as several additional bipartisan 5G security-related bills have passed in the House of Representatives. These include the House companion bill to Senator Cornyn's Secure 5G and Beyond Act, co-sponsored by Senators Sullivan and Blackburn of this Committee and others, which would require the U.S. to develop a 5G security strategy. Passage of such measures in the Senate would help demonstrate the U.S. commitment to 5G security to countries around the world grappling with these issues.
>
> (2) Support actions to accelerate 5G deployment. As I discussed, Ericsson believes that accelerated U.S. 5G deployment will in turn protect the security of the 5G supply chain, a goal that can be achieved through (i) increasing spectrum availability, especially mid-band; (ii) putting in place reasonable, streamlined small cell siting rules; (iii) developing and deploying a skilled tower workforce; and (iv) ensuring effective incentives to encourage 5G deployment in rural areas. We commend the work being done in these areas and urge the Committee to take up proposals to advance 5G deployments in the U.S., such as the STREAMLINE Act introduced by Senators Thune and Schatz, which would preempt certain state/local small cell deployment regulation; the TOWER Infrastructure Deployment Act introduced by Senators Gardner and Sinema, which would require the FCC to set up an Advisory Council to look at tower workforce issues; and the Telecommunications Skilled Workforce Act recently introduced by Senators Thune, Tester, Moran, Peters, and Wicker, which would require cooperation among various agency heads to develop recommendations and guidance that would empower the U.S. to catch up on the workforce demands of the 5G era.
>
> (3) Continue to enable a secure and robust marketplace of trusted suppliers in the U.S. and globally. As I have discussed, one of the key priorities for 5G is to strengthen and ensure the viability of a competitive, dynamic, diverse, and robust marketplace of trusted and secure suppliers on a global level, much like what we already have in the United States, recognizing that global and domestic security are intertwined. Such a marketplace, involving trusted and secure companies like Ericsson, can counter other potential players that may pose threats to national security. The Committee should remain attentive to factors that might promote – or undermine – the development of this global marketplace.
>
> (4) Continue to hold hearings on the subject of 5G security. In Ericsson's view, hearings such as this one provide an important vehicle for highlighting what industry is doing to ensure a secure 5G world – and for maintaining pressure on industry to stay true to its security commitments. Such hearings can have a similar motivating impact on government actors with security responsibility within their respective jurisdictions around the world. Shining additional light on all of these efforts will make them more effective in ensuring a secure supply chain.

Intel Corporation Next Generation and Standards Corporate Vice President and General Manager Asha Keddy stated:

- The United States government has a valuable role to play in the 5G supply chain by encouraging and supporting the emergence of a vibrant and trusted ecosystem. Intel commends the work done in 2019 by the Department of Homeland Security's Supply Chain Risk Management task force and sees this type of public sector-industry collaboration as vital to identifying and solving important questions about technology supply chain. Likewise, the work done by the Commerce Department's National Institute of Standards and Technology (NIST), has been extremely helpful in creating common goals and frameworks for progress among policymakers and industry. Intel has been active in these and other efforts to offer its expertise and insight in addressing supply chain risks and mitigations.
- Given the potential of 5G to provide valuable benefits to American businesses and consumers, the United States government should take measures to help facilitate widespread 5G deployments. Intel has advocated extensively for mid-band spectrum. Mechanisms to encourage increased investments in 5G infrastructure and to facilitate continued innovation throughout the 5G ecosystem will be critical. We appreciate Congressional and Executive Branch interest in areas such as potential broadband infrastructure deployment funding,), and ways to spur innovation and deployments in 5G such as the USA Telecoms Act, which serves as a good starting point for further discussion.

Nokia Americas Chief Technology Officer Mike Murphy asserted

> It is critically important that policymakers understand what is actually done today to ensure component security, product security and post-sale security support before prescribing new regimes for testing or certification that could impose costs on your trusted suppliers without necessarily providing a security dividend. And that is where a supply chain security strategy really should begin, careful assessment of known risks and current industry practices. Actions the U.S. might consider should draw from areas only where gaps are perceived. In helping industry to be a constructive partner in this process, Nokia recommends the following:
>
> - Identify best practices in design for security, supply chain validation and post-sale support and encourage the adoption of those practices;
> - Rather than focus on countries of origin for component sourcing or manufacturing, specify the components or activities that give rise to the risk of exploitation or manipulation. Not all components and products create risk. Narrowing the focus to specific components or products with risk will assist suppliers in making critical and cooperative decisions with governments about supply chain activities.

Center for Strategic and International Studies Senior Vice President and Director of the Technology Policy Program Dr. James Lewis stated

- We often hear that 5G is a race the U.S. cannot lose. It sounds dramatic, but I am not sure what it means. I am sure, however, that if there is a race, we are not losing. The U.S. is well positioned to take advantage of 5G technology, just as it did with 4G. The difference this time is we have real competition, a competitor who is well resourced, with a strong technology workforce, and a long record of unscrupulous behavior. We face a dynamic competitor in China, and there are things the U.S. can do to strengthen both its security and its technological leadership. Congress can play an important role in this.
- The 5G issue has become politicized and this shapes reporting in unhelpful ways. Let's dispel some of the myths. First, the U.S. has not been rebuffed in Europe. In speaking to

colleagues in the UK and Europe, there is broad agreement with the U.S. on the risks of using Huawei. The UK action is best seen as a partial ban on Huawei. The UK has blocked Huawei from two thirds of their network and from being used in sensitive areas around government and military installations. They and other European countries are committed to maintaining supplier diversity and avoiding Huawei dominance. The U.S. needs to find ways to benefit from these shared concerns to develop secure telecommunications networks.

- Where there is disagreement is in how to manage risk. The U.S., Japan and Australia have banned Huawei technology in their networks. This is the only way to eliminate risk entirely. Those who advocate a partial ban argue that if properly implemented, it makes the risk of using Huawei manageable. Some European countries will copy the UK's decision. This provides the U.S. an opportunity to work with our allies to ensure that a partial ban reduces risk and there could be real advantages for the security of telecom networks and cybersecurity. The recently issued European Union 5G Toolbox provides a framework to guide policy in a way that, if implemented fully, would reduce China's use of telecom infrastructure for espionage and influence.
- A full ban is the best outcome for security. It is not, in the judgment of some of our allies, the best outcome for their economies. Germany, for example, faces a dilemma. If it bans Huawei, the Chinese have explicitly threatened to retaliate again German auto exports, and China is Germany's largest market -China is playing hardball. German car companies have reportedly asked Chancellor Merkel not to ban Huawei. However, if Germany uses Huawei, China's intent is to use espionage to hollow out the German industry, and in particular the auto industry. If countries ultimately choose a partial ban, we will need to work with them to ensure that it is well implemented.

House Hearing On Fake and Unsafe Online Products

The House Energy & Commerce Committee's Consumer Protection and Commerce Subcommittee held a hearing to address the rapid increase in fake and potentially unsafe goods being sold in online marketplaces like Amazon, e-Bay, or Craigslist. Democratic staff released a background memorandum before the hearing.

In late January 2020, the Department of Homeland Security (DHS) released a report required by a presidential memorandum regarding counterfeit and pirated goods in electronic commerce. DHS contended that its report "identified a set of strong government actions that DHS and other federal agencies can begin executing immediately to address a crisis that is undermining America's trust in e-commerce even as it is exposing the American public to undue and unacceptable risks…[and] has proposed a set of best practices for private sector stakeholders that DHS believes should be adopted swiftly." (*See the January 30 Technology Policy Update for more detail*).

A week after DHS issued its report, President Donald Trump signed Executive Order 13904 (EO) "Ensuring Safe & Lawful E-Commerce for US Consumers, Businesses, Government Supply Chains, and Intellectual Property Rights" that tasks a number of federal agencies with implementing the policy articulated by the Administration:

> It is the policy of the United States Government to protect consumers, intellectual property rights holders, businesses, and workers from counterfeit goods, narcotics (including synthetic opioids such as fentanyl), and other contraband now being introduced into the

> United States as a result of the recent growth in e-commerce. The United States Government must also protect the revenue of the United States from individuals and entities who evade customs duties, taxes, and fees.

The Government Accountability Office (GAO) published its most recent assessment of counterfeit and pirated goods in 2018 and found

> Counterfeit goods provide a lucrative market for criminal activity and can pose serious risks to consumers. Growth in e-commerce has changed the way counterfeiters interact with consumers, and the accompanying increase in the volume and sophistication of counterfeit goods has created challenges for U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) enforcement.

Chair Jan Schakowsky (D-IL) said the hearing would examine how counterfeit products and fake reviews are making Americans less safe at home, at work, and on the road. She remarked that in planning the hearing she had two clear goals in mind: 1) to strengthen the existing Consumer Product Safety Commission's (CPSC) relationship with the U.S. Customs and Border Patrol (CBP) to keep counterfeit and unsafe products from entering the U.S.; and 2) to examine what tools the Federal Trade Commission (FTC) needs to combat the proliferation of fake reviews online since recent cases like its settlement with cosmetic company Sunday Riley clearly demonstrates that it's not currently up to the task of taking on some of the worst problems.

Schakowsky stated that shortly after planning began for the hearing, she was pleased to learn that the Trump Administration's plan to combat counterfeits entering the marketplace under the leadership of Dr. Peter Navarro. She added that she expects the Administration to partner with the subcommittee in an effort to strengthen CPSC's relationship with customers. Schakowsky stated that the vast majority of the commerce shipped to the U.S. skirts normal customs procedures and often almost all inspections are waived under a de minimis waiver. She claimed that worse still, Dr. Nancy Beck's nomination leaves her less hopeful for collaboration given Beck's anti-consumer record at the Environmental Protection Agency (EPA) and as an executive at the American Chemical Council.

Schakowsky stated these problems neither begin nor end at ports of entry. She contended that fake reviews are becoming more and more widespread and up to this point, the FTC has proven that it needs more tools to combat this growing concern by consumers. Schakowsky said organized retail crime such as selling counterfeits and stolen products poses a threat to consumers who are unwittingly purchasing these items in online marketplaces. She argued the emergence of these unregulated platforms has given criminal enterprises additional avenues to sell stolen and counterfeit goods to unsuspecting consumers. Schakowsky asserted online marketplaces need to place safety and accountability to consumers before profits. She remarked that unfortunately there are more and more companies characterizing online commerce as content seeking to use the liability shield in Section 230 of the Communications Decency Act, a law badly in need of reform. Schakowsky claimed that matters are made worse by the Administration's policy to further enshrine Section 230 by exporting it in trade agreements all over the world. She noted her letter written the week before the hearing to Ambassador Robert Lighthizer in which she, Chairman Frank Pallone Jr (D-NJ), and Ranking Member Greg Walden (R-OR) asked the Administration to omit Section 230-type language from future trade agreements, and she pledged to continue working towards this goal. Schakowsky concluded by stating her interest in hearing from the

witnesses on the current state of play and how policymakers can improve the situation by arming the CPSC and the FTC with the tools necessary to root out this problem.

Ranking Member Cathy McMorris Rodgers (R-WA) said that I want to first recognize how President Trump and his Administration are leading to combat counterfeit and pirated goods online. She asserted that the President has made this a priority, which is clear in "Phase 1" of the U.S.-China Trade deal. McMorris Rodgers stated that for instance, China agreed to:

- Provide enforcement procedures to facilitate effective and quick takedowns;
- Consider revoking e-commerce operating licenses for repeated failures;
- Take action to stop the manufacturing of pirated and counterfeit products;
- Take enforcement action against counterfeit medicines and other products that may have a significant impact on public health or safety; and
- Increase the number of trained professionals to inspect, detain, and destroy any counterfeit goods found at the Chinese border.

McMorris Rodgers added that DHS released its first report required by President Trump's April 2019 Memorandum on Combating Trafficking in Counterfeit and Pirated Goods, a call to action to fight against cheaters and bad actors gaming the e-commerce system. She claimed that the report recommends where the government should take action, and best practices for e-commerce platforms and other third-party marketplaces.

McMorris Rodgers stated that among the best practices, the Administration is calling on companies to:

- enhance the vetting of third-party sellers;
- limit high-risk products;
- clear transactions through banks that comply with U.S. law; and
- provide rapid notice and takedown procedures.

She noted that following the report, President Trump signed an executive order to ensure safe and lawful e-commerce protects people and guards against intellectual property abuse.

McMorris Rodgers claimed the Administration should be commended for their leadership, and as I've said before, to win the future and beat China, America must be the global leader in the 21st-century economy. McMorris Rodgers asserted that just like we must lead to promote artificial intelligence and deploy autonomous vehicles, America must also lead to stop counterfeit goods and protect our intellectual property. She argued that if we do not step up, China will dictate the terms and rules for the future, and the Chinese Communist Party will win with the playbook they've always used: by undermining human rights, stealing from our innovators, and cheating and harming Americans.

McMorris Rodgers contended that America innovates and creates, while China cheats and steals. She cited an Organization for Economic Cooperation and Development report that found China is the "single largest producing market" of counterfeit and pirated products. McMorris Rodgers stated that Administration officials estimate that more than 100,000 packages from China arrive in America a day that could harm and defraud people, and more than 85 percent of all contraband seized at our borders come from China and Hong Kong.

McMorris Rodgers stated that while the Administration is taking decisive action, the government and regulations cannot solve this issue alone because the best way to predict the future is to

invent it. She claimed that American innovators must be equipped to win the future and beat China in artificial intelligence, blockchain, Internet of Things (IOT), and other emerging technologies. McMorris Rodgers stated that companies today are leveraging AI to analyze data points to discover counterfeit listings and repeat offenders, IOT provides identification and traceability functions that can be used to address and track counterfeit sales, and blockchain may provide a unique solution to this complex problem too.

McMorris Rodgers stated that for example, a tamper-proof chain of custody that uses smart tags can ensure only authentic products are included on the blockchain and sold. She added that as the DHS report suggests, we should leverage public-private partnerships to develop a national awareness campaign, and we should educate people about the risks of counterfeits, as well as the various ways they can spot and report counterfeits online.

Amazon Vice President Dharmesh Mehta stated stated that "[p]artnerships with other retailers, social media companies, law enforcement, the Executive Branch, and Congress are critical to holding bad actors accountable and driving counterfeits and unsafe products to zero. To strengthen collaboration and cooperation and improve the fight against counterfeits and unsafe products for consumers, Amazon suggests the following additional actions:

- ***Improve bad actor information sharing among stores and other service providers***. Amazon supports the creation of a private information exchange that will enable industry participants to better identify and stop bad actors of all types before they can reach consumers. Bad actors are collaborating with each other; we believe industry should find ways to share risk signals to help strengthen each other's defenses.
- ***Enhance criminal prosecution of intellectual property crimes***. Amazon supports the Department of Justice prioritizing prosecution of intellectual property crimes in order to deter perpetrators. In 2017, only 0.1% of filed federal criminal cases involved charges for trafficking in counterfeit goods, and 56% of counterfeiters sentenced that year received no jail time. As a result, there is often little disincentive for bad actors in committing IP crimes. Increased criminal prosecution alone will not solve the problem of counterfeiting, but more funding for law enforcement and more severe penalties for convictions are essential to winning this fight.
- ***Improve information sharing from Customs***. Amazon encourages Customs and Border Protection (CBP) to facilitate mutually beneficial partnerships that will help provide increased visibility and transparency into shipments. Specifically, CBP should provide us with identifying information for every counterfeit-based seizure bound for an Amazon fulfillment center. When CBP seizes such packages, there might be similar products from the same bad actor sitting in Amazon's warehouses. Sending a picture of the "FBA number" found on the outside of each such package will help us protect our customers and the intellectual property of rights owners by removing related products and associated bad actors from our stores.
- ***Require sharing of pre-arrival data on all small packages***. Amazon supports a Customs requirement that every package imported into the United States provide advance electronic data to CBP to allow better targeting of suspected counterfeits. Currently, no cohesive data tracking system exists for postal shipments, and bad actors from outside the United States are able to hide their identities and avoid detection. Enforcement of these requirements, and the data derived from them, will help law enforcement identify bad actors and allow Amazon to better protect customers and rights owners.

Apple Intellectual Property Senior Director Jeff Myers explained

> Today, criminals increasingly use online third-party marketplaces to sell counterfeit Apple products. Fraudsters use Apple's name, logos, designs, and marketing images in their online offers to deceive customers into believing that fake Apple products are the real thing. Even after making a purchase, customers might be unaware that they purchased a fake product, and when that product does not meet Apple's high standards for safety and performance, it diminishes customers' trust in the quality of Apple's products and can have serious safety implications.

Myers stated that "[w]e agree with many of the best practices outlined in the recent reports from the Senate Finance Committee and the Department of Homeland Security, including the following:

- First, marketplaces should do a better job vetting sellers to ensure that they are real, reputable companies that will stand behind the goods they sell. If a seller can't pass simple vetting requirements, they should not be allowed on the marketplace.
- Second, marketplaces should adopt better policies to address repeat offenders and kick them off marketplaces for good.
- Third, marketplaces should offer customers more information about the identity of sellers on offer pages, or they could provide notifications when they learn that a seller was supplying counterfeits.
- Fourth, marketplaces should work more closely with companies like Apple and law enforcement to bring criminal actions against counterfeiters. We have done this with some marketplaces, and we appreciate those efforts.
- Finally, there should be greater proof of authenticity requirements for certain categories of products where counterfeits comprise a significant portion of what is sold, particularly if safety concerns are present."

Consumer Reports Vice President David Friedman stated "[t]o ensure that the digital marketplace lives up to the true potential of the internet and a well-functioning market, two fundamental changes are required:

- First, online marketplaces must have sufficient incentives to put consumers first by aggressively policing their platforms for dangerous products, counterfeits, and false, misleading, or manipulative information. As a baseline, these incentives should be evaluated against the level of incentives they would face in the physical market and then be further strengthened or otherwise adjusted to account for the complexity and pace of change in digital commerce.
- Second, government agencies must focus on finding problems, holding bad actors accountable, and adjusting the rules to address existing challenges and anticipate new ones. These agencies also need to be sufficiently resourced, in terms of personnel, budget, and authority to carry out this critical work.

Friedman highlighted Recommendation 1:

> Change the incentives for platforms in the digital marketplace. The various problems outlined in this testimony would not exist if all e-commerce platforms supported robust, honest markets and tried to succeed, first and foremost, by truly meeting the needs of their users. At some level, platforms clearly have an interest in consumers trusting their marketplaces, but the existence of dangerous and counterfeit products, fake reviews and manipulative practices make clear that, currently, platforms do not have sufficient incentives to deploy resources to prevent abuse of their services. Indeed, in some cases,

they are perversely incentivized to permit illegal behavior because it increases their profits.

Friedman explained Recommendation 2: Strengthen the Consumer Product Safety Commission, Federal Trade Commission and the National Highway Traffic Safety Administration (NHTSA):

The CPSC, FTC, and NHTSA are critical agencies that play a significant role in protecting U.S. consumers despite lacking the resources they would need to carry out all that they are capable of doing using their existing authorities. For example, the CPSC, FTC, and NHTSA all have about half as many people working for them today as 1980; meanwhile, the economy has tripled in size. All three agencies should receive far greater funding and staff—at least doubling each of their current budgets for research, rulemaking, and enforcement—and should take the following steps to further bolster their work:

- Update federal rules to account for current and future ways consumers shop for products, which includes addressing the growth of e-commerce and direct international shipments and incentivizing the adoption of best practices by online marketplaces;
- Work with Customs and Border Protection to assess imports by potential risk to consumers and stop entry of hazardous products to the U.S. market;
- Monitor the domestic market for available unsafe products, misleading and deceptive practices, and inadequate online marketplace or retail controls that could put consumers at greater risk;
- Publicize online marketplace hazards of which they are aware; and
- Enforce federal safety laws and regulations to deter wrongdoing.

Congress should specifically enhance the FTC's ability to police the modern economy by:

- Expand the Commission's powers to include the authority to directly levy civil penalties and promulgate rules under the Administrative Procedure Act;67
- Clarifying that Section 5 of the FTC Act bars fake reviews and extends to more indirect promotion such as paid followers, likes, reposts, and types of engagement that distort the marketplace for goods and services.

Public Citizen Global Trade Watch Director Lori Wallach stated that "[g]iven the scope and scale of threats posed to consumer health and safety in the current e-commerce environment, and the way in which those threats are generated by different factors, remedies will require changes on at least two levels."

1. Government actions

- CPSC: The rapid rise of e-commerce poses new challenges for CPSC since the agency does not currently have the capability to police de minimis e-commerce that enters the United States as well as it can police high-value commerce. The agency's legal, operational and resource constraints will need to be addressed. It must have the authority to hold accountable all of the parties in the e- commerce supply chain that are implicated in importing non-compliant products. CPSC's Office of Import Surveillance requires the funding to create and staff effective inspection systems that expand their presence to ensure the CPSC mission can be successful in an e-commerce context that is different in many ways from the large-value import regime to which it is now adapted, including with respect to where additional inspection staff must be fielded and new data or better data sharing between agencies developed to effectively target high-risk imports.
- FTC: The Federal Trade Commission has existing authority over unfair and deceptive practices and retail mislabeling. It is unconscionable that the FTC has not acted to discipline the big online marketplaces that claim they are not legally responsible for deceptive content on their sites, facilitate the sale of goods falsely labeled as meeting

regulatory approvals or third-party certifications inspection, and in some instances do not even deliver the products presented to the consumer online. The findings of the Wall Street Journal investigation summarized earlier in this testimony provide a rich vein for FTC action, if the agency cares to engage in its mission.

- CBP: CBP has the statutory authority to inspect *any* package as it is imported into U.S. territory. Yet the agency is sitting on two slightly conflicting regulations and choosing to operate in a manner that ensures that de minimis shipments are not subject to the basic data filing requirements that would allow U.S. government agencies responsible for consumer health and safety to target high risk goods. The pilot program for de minimis goods discussed previously in this testimony is a voluntary program, not a resolution to the data dodge now facilitating uninspected entry of e- commerce imports that pose high risks to consumers. As well, CBP should use its existing authority to require formal Entry for de minimis goods that it deems a high risk of evading compliance with any law or regulation. CBP has broad authority it must employ to stop and prevent the trafficking of counterfeit goods, from the assessment of civil fines and other penalties to debarring and suspending irresponsible actors. It also can and should require bonding for high- risk goods. Many of these authorities are underutilized or underdeveloped to match the risks in the evolving e-commerce environment.
- Legislating a definition of e-commerce seller: Congress must put an end to the sham of world-class retailers claiming not to be sellers and thus dodging accountability for conduct that puts consumers' health and safety at risk and unfairly penalizes legitimate businesses.

2. E-Commerce Retailers

- Actions by companies in the e-commerce supply, distribution and sales chain will be necessary to reduce the heavy volume of counterfeit, dangerous goods to which U.S. consumers are now being exposed thanks to growing online sales. As the recent CBP report noted: "Absent the adoption of a set of best practices and a fundamental realignment of incentives brought about by strong government actions, the private sector will continue to fall far short in policing itself. Indeed, the current incentive structure tends to reward the trafficking in counterfeit and pirated goods more than these incentives help to deter such trafficking." Many of the practices it recommends could reduce the platforms' facilitation of sales of fake and unsafe goods.
- **Significantly Enhanced Vetting of Third-Party Sellers and Requirement of Insurance or Bonding or Other Forms of Security as a Condition of Access:** Platforms should only allow third-party sellers that have been vetted and approved based on a uniform assessment and proof of insurance to indemnify consumers for harm caused by their products. Assessments should include sufficient identification of the seller, its accounts and listings, and its business locations prior to allowing the seller to list products on the platform; certification from the seller as to whether it, or related persons, have been banned or removed from any major e-commerce platforms, or otherwise implicated in selling counterfeit products online or selling unsafe products; use of technological tools, as well as analyses of historical and public data, to assess risk of sellers and products; and establishment of an audit program for sellers, concentrating on repeat offenders and those sellers exhibiting higher risk characteristics. Any failure to provide accurate and responsive information should result in a determination to decline the seller account and/or to hold the seller in violation of the platform's terms of service.
- **Pre-Sale Identification of Third-Party Sellers and the Rule of Origin of the Good for Sale:** Providing consumers with this information up front as part of the first screen available for a product is critical for consumers to make informed choices.

- **Set and Enforce Limitations on High Risk Products:** Platforms should have in place protocols and procedures to place limitations on the sale of products that have a higher risk of posing threats to public health and safety. For example, some major platforms completely prohibit the sale of prescription medications by third-party sellers in their marketplaces. Many platforms also ban the sale of products that are known to pose a safety risk when sold online. Examples include car airbag components, infant formula and new batteries for cellphones. But these terms, which are included on platforms on which prohibited and restricted goods regularly appear, are only effective if enforced by the platform through an investment in regular surveillance and monitoring and the development of automated tagging systems that keep unsafe products from reappearing on sites.
- **Effective Takedown Procedures for Unsafe Goods:** Platforms should create and maintain clear, precise, and objective criteria that allow for quick and efficient notice and takedowns for unsafe goods and protocols to ensure goods are not relisted.

Washington State Privacy Bill Dies

The Washington State Senate and House failed to reach agreement on a final version of the "Washington privacy act" (SB 6281) and have adjourned for the rest of 2020, meaning that privacy legislation is almost certainly not going to be enacted in this year. Consequently, the "California Consumer Privacy Act" (CCPA) (AB 375) essentially stands alone as the only major state privacy stature at present. The House's insertion of a private right of action and tightening some of the provisions as called for by privacy and consumer advocates seems to have been the differences that were too vast to close given the amount of time lawmakers had. And yet, a privacy bill made it farther than last year when the Senate's bill perished in the House without even coming to the floor for a vote, largely over facial recognition provisions. However, it looks like lawmakers will try again next year when the Washington state legislature is slated to be in for most of the year unless, of course, Congress passes a federal privacy law that preempts state laws.

A number of stakeholders in the legislature sought to make clear where they think the blame should be laid for SB 6281 failing to make it to the governor's desk. In a statement, one of the Senate's primary sponsors, Senator Reuven Carlyle (D-Seattle) claimed that "[t]he impasse remains a question of enforcement...[and] I continue to believe that strong attorney general enforcement to identify patterns of abuse among companies and industries is the most responsible policy and a more effective model than the House proposal to allow direct individual legal action against companies."

In her framing of SB 6281 dying, the House Innovation, Technology and Economic Development Committee Ranking Member Norma Smith (R-Clinton) claimed that the version of the bill the Senate passed "purported to be comprehensive consumer data privacy...[but] was corporate-centric, not consumer focused." She added that the House "closed some of the most significant loopholes and provided individual consumers the ability to access justice should their rights—as declared in the bill—be violated." Smith argued that "the Senate wanted both big loopholes and weak enforcement...[a]nd that is why the bill died today."

Third Set of Draft CCPA Regulations Released For Comment

The California Attorney General's Office (OAG) has released a third iteration of draft regulations to implement the "California Consumer Privacy Act" (CCPA) (AB 375) and is accepting comments by email or U.S. mail until 5:00 pm PDT on March 27 (*See here for a clean copy and here for a redline*.) Of course, the CCPA requires that regulations be in place by July 1, 2020.

The OAG explained that it "first published and noticed the proposed regulations for public comment on October 11, 2019...[but] [o]n February 10, 2020, the Department gave notice of modifications to the proposed regulations, based on comments received during the 45-day comment period." The OAG stated that it "received around 100 comments in response to the modifications...[and] [t]his second set of modifications is in response to those comments and/or to clarify and conform the proposed regulations to existing law."

Most of the changes are marginal. However, there a few notable modifications. Among the notable deletions, the OAG removed the section with an illustration on what an acceptable opt-out toggle button might look like. Additionally, the revised draft regulations strike the section that clarifies what could qualify as "personal information" that triggers many of the responsibilities and obligations under the CCPA.

In terms of new language, the draft regulations make clear that regarding a business's notice responsibilities, "[a] business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information." Additionally, an entity's privacy policy regarding a person's right to know about personal information collected, disclosed or sold must contain two additional items:

- the categories of sources from which the personal information is collected. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.
- the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.

EARN IT Act Finally Introduced

Senate Judiciary Committee Chair Lindsey Graham (R-SC), Ranking Member Dianne Feinstein (D-CA), and Senators Richard Blumenthal (D-CT), Josh Hawley (R-MO) formally introduced legislation they floated earlier this year that could potentially result in the liability shield enjoyed by technology being removed. Critics claim the legislation is an attempt to force technology companies to either give up end-to-end encryption or build in backdoors to encryption that will ultimately compromised. If enacted, the EARN IT Act would represent a second piece of legislation to change Section 230 of the Communications Decency Act in the last two years with enactment of "Allow States and Victims to Fight Online Sex Trafficking Act of 2017" (P.L. 115-164).

The "Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020" (EARN IT Act of 2020) (S.3398) would establish a National Commission on Online Child Sexual Exploitation Prevention (Commission) that would design and recommend voluntary "best practices" applicable to technology companies such as Google, Facebook, and many others to address "the online sexual exploitation of children." The Department of Justice (DOJ) would name the chair of the Commission and the Department of Homeland Security (DHS) and Federal Trade Commission (FTC) would each name one member of the Commission with the Speaker of the House, House Minority Leader, Senate Majority Leader and Senate Minority Leader each being able to

appoint four members each. The Commission would submit its best practices to the Attorney General within 18 months of being convened, and if approved by DOJ, with the concurrence of DHS and the FTC, would publish these voluntary standards. Moreover, the EARN IT Act contains language allowing for the fast track consideration under which Congress could codify these practices, and thereafter technology companies subject to these standards would need to submit annual certifications that it "has a reasonable basis to conclude that review does not reveal any material non-compliance with the requirements of the best practices." If a technology knowingly submits a false certification, then the company and the responsible executives and employees would face criminal liability, including fines and imprisonment. The bill would remove the liability shield under Section 230 of the Communications Decency Act with respect to state child exploitation laws unless companies either certify compliance with either the Commission's best practices or those enacted by Congress or through the use of alternative reasonable measures.

In their press release, Graham, Feinstein, Blumenthal, and Hawley asserted:

> The EARN IT Act is supported by more than 70 groups, survivors and stakeholders, including the National Center for Missing & Exploited Children (NCMEC), Rights4Girls, and the National Center on Sexual Exploitation.
>
> Background on the EARN IT Act:
>
> - In July 2019, the Senate Judiciary Committee held a hearing titled, "Protecting Innocence in a Digital World".
> - Later in 2019, the New York Times published a series of investigative reports, describing the rapid increase of child sexual abuse material on prominent online platforms. This is a threat that has not received a consistent and forceful response from the tech industry.
>   - Reports of suspected child sexual abuse material to the NCMEC CyberTipline have exploded since its inception. For example, over the past five years, reports increased from 1.1 million in 2014 to 16.9 million covering 69.1 million photos, videos, and files in 2019.
> - Section 230 of the Communications Decency Act gives "interactive computer services" significant immunity from civil liability, as well as state criminal liability for third party content on their platforms. Sadly, given this limited liability, many companies do not aggressively go after online child sexual exploitation.

Among those opposed to the bill are:

- Johns Hopkins University Associate Professor Matthew Green argued the EARN IT Act "represents a sophisticated and direct governmental attack on the right of Americans to communicate privately…[and] I can't stress how dangerous this bill is, though others have tried."
- The Electronic Frontier Foundation (EFF) asserted of the bill that "its supporters' strategy is clear. Because they didn't put the word "encryption" in the bill, they're going to insist it doesn't affect encryption….It's true that the bill's authors avoided using that word. But they did propose legislation that enables an all-out assault on encryption."
- The Center for Internet and Society at Stanford Law School claimed the EARN IT Act "aims to kneecap encryption under the guise of protecting children online, while capitalizing on the techlash and the current unpopularity of Section 230 of the Communications Decency Act."

The EARN IT Act was introduced the same day the Departments of Justice (DOJ) and Homeland Security (DHS) announced the release of the Voluntary Principles to Counter Online Child Sexual

Exploitation and Abuse developed in conjunction with the governments of Australia, Canada, New Zealand, and the United Kingdom. DOJ and DHS claimed in their press release that

> The voluntary principles provide a common and consistent framework to guide the digital industry in its efforts to combat the proliferation of online child exploitation. The voluntary principles cover the following themes:
>
> - Prevent child sexual abuse material;
> - Target online grooming and preparatory behavior;
> - Target livestreaming;
> - Prevent searches of child sexual abuse material from surfacing;
> - Adopt a specialized approach for children;
> - Consider victim/survivor-led mechanisms; and
> - Collaborate and respond to evolving threats.

DOJ and DHS added

- These voluntary principles are built on existing industry efforts to combat these crimes. Some leading companies have dedicated significant resources to develop and deploy tools in the fight to protect children online and to detect, disrupt and identify offenders. Although significant progress has been made, there is much more to be done to strengthen existing efforts and enhance collective action.
- These principles are intended to have sufficient flexibility to ensure effective implementation by industry actors. Some companies have already implemented measures similar to those outlined in these principles. Regardless of whether or not a company chooses to adopt these principles, existing laws and regulations in relevant jurisdictions continue to apply to all companies. Nothing in these principles overrides or is contrary to the need for companies to comply with the law.

These voluntary principles on online child abuse and exploitation are of a piece with previous efforts by the DOJ and Attorney General William Barr to pressure technology companies to provide greater technical assistance to defeat end-to-end encryption.

A week later, at a hearing, the Senate Judiciary Committee looked at the EARN IT Act with Graham and Blumenthal making opening statements of their bill. Many of the Members expressed support for the legislation or its goals and argued that large technology companies have simply not been doing enough to combat online child exploitation.

National Center for Missing & Exploited Children (NCMEC) Vice President John Shehan stated

> The EARN It Act is a child protection bill that addresses many of the gaps identified by NCMEC in this written testimony regarding current efforts to combat the proliferation of child sexual abuse and exploitative material online, including:
>
> (1) lack of adoption of consistent practices and technology across the tech industry to combat the problem;
>
> (2) failure of companies to implement best practices across all of their platforms and services;
>
> (3) reliance on wholly voluntary measures to protect children from being enticed/groomed online for sexual abuse and to prevent images of their rape and sexual abuse from circulating online;

(4) absence of incentives for ESPs to invest and engage in best practices to keep children safer online; and
(5) denial of a child victim's right to his or her day in court against all parties, including tech companies, that have recklessly contributed to the child's revictimization when sexually abusive images are recirculated online.

The EARN It Act addresses each of these gaps, shortcomings, and inconsistencies.

Match Group Chief Legal Officer & Secretary Jared Sine explained

- Match Group takes the privacy of our users seriously, which is why we have developed a privacy framework that meets the standards of the GDPR—and all are brands are required to meet or exceed these standards. Like all internet companies, we grapple with the same inherent tensions that exist between privacy and security.
- We believe that these issues are not mutually exclusive, especially when it comes to our support of the EARN IT Act. There are technological solutions to balance safety for our children and privacy, and we need to work to enable the Commission and develop those solutions. That is the point of the Commission—its ability to collaborate to solve these issues, taking into account the ecosystem, its needs, and the rights of its users and providers to drive a solution that works for everyone.
- We also believe that Section 230 has been a critical part of the internet's rise and success and must be kept strong and vibrant. However, we do not believe that companies who do nothing to stop child exploitation should receive the benefit and trust that Section 230 has long granted them.
- This legislation acknowledges the importance of Section 230 to privacy, free speech, and so many other rights that we hold dear, while rightfully recognizing that online platforms must do more. The bill also creates a collaborative framework for setting standards across the internet ecosystem that will help tech companies fulfil their moral and societal obligation to protecting our kids online.
- We do not take our support for this proposal lightly. We recognize how important it is to strike the right balance between privacy and security. But we believe the proposed legislation has the ability to do just that: by balancing those needs of safety and privacy through collaboration. As part of the standard setting process, the Commission established by the EARN IT Act must be empowered and instructed to take these tensions into account.
- Match Group strongly supports the Commission included in this proposal for the very reason that it provides a forum for bringing law enforcement, industry, and technical experts together to create commonsense rules of the road that will not just level the playing field for technology companies but also incentivize investing in—and enforcing—online safety. Not only do we support this legislation, but we'd also like to offer suggestions to make it even stronger. We share your goal of making sure this is done in a way that does not stifle innovation but still has teeth, a topic I know Sen. Graham and others have talked about already.

The Catholic University of America Professor of Law Mary G. Leary explained that

- As Congress contemplates the appropriate limits of Section 230 in the space of child sexual abuse material (CSAM) more generally, particular attention should be paid to this issue and its history. In the current form of the EARN It Act, an interactive computer service can claim a safe harbor from both state enforcement of its criminal laws and civil action through two fairly easily attainable paths. First, it obtains broad immunity if an officer

certifies that the provider conducted a thorough review of the implementation and operation of the best practices and he has a "reasonable basis to conclude that review does not reveal any material non-compliance" with the best practices. This should be understood to be a relatively low standard not establishing actual compliance with best practices. This is particularly true given that the best practices will be generated by a commission whose membership largely comes from the tech community or its allies. Such a certification – which notably does not certify the entity is, in fact, in compliance with the practices - will provide the entity immunity from civil suit or state level prosecution. This exclusive protection is sweeping, and yet available to it for a very qualified certification. While the provider does risk prosecution, such a risk is remote as prosecution can only occur if it can be established that the provider knowingly submitted a false certification. The variance between the mens rea necessary for certification (reasonable basis to not believe there is material non- compliance) and that necessary for prosecution (knowingly submitting a false statement) is significant.

- The second path to immunity is a provider establishing that it has implemented "reasonable measures" to prevent it from being used for the exploitation of minors. This will require a trial court, possibly at a motion to dismiss stage, to determine if the provider was reasonable in its measures. Such an approach risks a similar outcome as with the aforementioned Section 230 sex trafficking caselaw in which courts, unfamiliar with the technology and relying on outdated precedent, arguably expanded Section 230 immunity further than congressionally intended.
- In such a regime, a victim survivor can attempt to hold a provider responsible for its actions and file a suit with facts and a good faith belief that the provider violated the law, was not in compliance with the practices, and, in fact, did not make a certification in good faith. Yet, by Section 230 immunity being awarded to the provider at such a low standard, the risk exists that the case will be dismissed prior to discovery. Thus, the legal landscape that led to Backpage successfully avoiding liability for several years could be repeated. That is to say an actor could be engaged in activity for which liability is appropriate, but a victim survivor is precluded from proving that case due to the sweeping scope of such immunity available to providers merely by arguing they are reasonable or that they had no reason to believe a material non-compliance occurred.

Internet Association (IA) Deputy General Counsel Elizabeth Banker contended that

IA is concerned that the EARN IT Act would burden, discourage, or even prevent, ongoing efforts by internet companies to keep their platforms safe and to identify and remove abusive content. It also would undermine the efforts of law enforcement, and nongovernmental organizations like NCMEC, to hold bad actors to account and combat child sexual abuse material (CSAM) online.

1. The bill would be vulnerable to Fourth Amendment challenges that could render evidence from platforms' screening efforts inadmissible, therefore hampering efforts to combat CSAM. Criminal defendants across the United States have filed motions to suppress evidence of child sexual exploitation crimes in the hopes of avoiding conviction.4 The argument that many of these criminal defendants make is that providers, including IA member companies, who proactively detect CSAM and who report it to NCMEC's CyberTipline, act as "agents of the government" for Fourth Amendment purposes. Under Fourth Amendment jurisprudence, a search performed by an agent of the government is subject to the same requirements as if the government performed the search directly. If a criminal defendant is able to show that the search violated the Fourth Amendment, the

exclusionary rule may require that the evidence obtained through the illegal search, and any fruits of the poisonous tree, be excluded at trial.

2. The bill would delegate authority to set important standards to an administrative body. The EARN IT Act would delegate important decisions concerning security, privacy, and free speech on the internet—weighty and complex matters that directly impact hundreds of millions of consumers—to an administrative body that would be composed of members who are not elected representatives and that would operate with little transparency. These critical decisions should not be made through an opaque process; rather, they should be made by Congress directly.

3. The bill would be vulnerable to First Amendment challenges. If the EARN IT Act became law, it would be vulnerable to various First Amendment challenges. IA is concerned that such vulnerabilities create legal jeopardy, significant delays, and other costs and impediments that would inevitably slow the achievement of the goals that everyone engaged in the fight against CSAM is trying to attain.

Further Reading

- "Coronavirus consumes tech: The latest from an industry in turmoil" – *Protocol*
- "What Are My Photos Revealing About Me?" – *The Markup*
- "Pentagon to Take Corrective Action on JEDI" – *Nextgov*
- "We Built a Database of Over 500 iPhones Cops Have Tried to Unlock" – *Motherboard*
- "Intelligence Officials Temper Russia Warnings, Prompting Accusations of Political Influence" – *The New York Times*
- "As the U.S. spied on the world, the CIA and NSA bickered" – *The Washington Post.*
- "5 years of Intel CPUs and chipsets have a concerning flaw that's unfixable" – *Arc Technica*
- "Throwing away the throwaway society" – *Politico*
- "No Cell Signal, No Wi-Fi, No Problem. Growing Up Inside America's 'Quiet Zone'" – *The New York Times*
- "Twitter CEO Jack Dorsey gets to keep his job — for now" – *Recode*
- "Why All the Warby Parker Clones Are Now Imploding" – *Marker*