Cyber Update
19 February 2019
By Michael Kans

DHS Cyber Funding In Funding Package

Congress agreed on a package that the President signed to fund those agencies operating under a continuing resolution (CR) for most of fiscal year (FY) 2019 to date. The "Consolidated Appropriations Act, 2019" (H.J.Res.31) provides a total of $63.315 billion for the Department of Homeland Security in Division A (as compared to the enacted total for FY 2018 minus appropriations for emergencies and disasters of $56.928 billion). The new Cybersecurity and Infrastructure Security Agency (CISA) would receive less funding than National Protection and Programs Directorate (NPPD) received the previous year ($1.682 billion for the current year versus an enacted level of $1.911 billion for FY 2018) with $782 million for cybersecurity operations and support, of which $272 million would be provided for the National Cybersecurity and Communications Integration Center (NCCIC) and $463 million for "Federal Cybersecurity," which includes the Continuous Diagnosis and Mitigation (CDM) program and National Cybersecurity Protection System (NCPS).

In the Joint Explanatory Statement, the Appropriations Committees included a number of requirements:

- CISA is directed to provide a briefing, not later than 90 days of the date of enactment of this Act and semiannually thereafter, on the updated timelines and acquisition strategies for the National Cybersecurity Protection System (NCPS) program and the Continuous Diagnostics and Mitigation (CDM) program, including the accelerated deployment of CDM Phase 4 data protection management (Digital Rights Management, Data Masking, Micro-Segmentation, Enhanced Encryption, Mobile Device Management, etc.) across all ".gov" civilian agencies.
- Advanced persistent threats targeting critical infrastructure sectors in the United States is cause for concern. Not later than 60 days of the date of enactment of this Act, the Department is directed to brief the Committees on the status of implementing the recommendations of the 2017 report of the National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*.
- In July 2018, the Secretary announced the redesignation of the Office of Cyber and Infrastructure Analysis (OCIA) as the National Risk Management Center (NRMC) in an effort to refocus risk management efforts across the various critical infrastructure sectors. As part of the effort, CISA aims to improve

> security and resiliency outcomes by focusing more on sector-wide and cross-sector risks and dependencies. The conferees include a realignment of $17,216,000 into this PPA for such activities. Not later than 90 days after the date of the enactment of this Act, the NRMC is directed to provide a detailed spend plan for its fiscal year 2019 activities.

GAO Calls For FTC Authority To Levy Civil Fines

The Government Accountability Office (GAO) has released a report that "focuses on Internet data privacy, which is affected by the collection and use of consumers' personal information such as their Internet browsing histories, purchases, locations, and travel routes." The GAO interviewed stakeholders in industry (including Apple, Facebook and Google), academia, and former government officials (many of them former Federal Trade Commission (FTC) and Federal Communications Commission (FCC) officials.) The GAO noted "[r]ecent developments regarding Internet privacy suggest that this is an appropriate time for Congress to consider comprehensive Internet privacy legislation." The GAO concluded that a federal privacy statute could strengthen enforcement effort of consumer privacy, provide certainty to the marketplace that would foster greater innovation and product development, and foster great assurances for consumers their privacy will be protected. These recommendations could come to be seen as a centrist position on what a federal privacy statute should be.

The GAO explained that "[s]takeholders identified three main areas in which Internet privacy oversight could be enhanced:

- *Statute*. Some stakeholders told GAO that an overarching Internet privacy statute could enhance consumer protection by clearly articulating to consumers, industry, and agencies what behaviors are prohibited.
- *Rulemaking*. Some stakeholders said that regulations can provide clarity, enforcement fairness, and flexibility. Officials from two other consumer protection agencies said their rulemaking authority assists in their oversight efforts and works together with enforcement actions.
- *Civil penalty authority*. Some stakeholders said FTC's Internet privacy enforcement could be more effective with authority to levy civil penalties for first-time violations of the FTC Act.

The GAO stated that "[a]lthough FTC has been addressing Internet privacy through its unfair and deceptive practices authority, among other statutes, and other agencies have been addressing this issue using industry-specific statutes, there is no comprehensive federal privacy statute with specific standards." The GAO added that

> Debate over such a statute could provide a vehicle for consideration of the Fair Information Practice Principles, which are intended to balance privacy

> concerns with the need for using consumers' data. Such a law could also empower a specific agency or agencies to provide oversight through means such as APA section 553 rulemaking, civil penalties for first time violations of a statute, and other enforcement tools. Comprehensive legislation addressing Internet privacy that establishes specific standards and includes APA notice-and-comment rulemaking and first-time violation civil penalty authorities could help enhance the federal government's ability to protect consumer privacy, provide more certainty in the marketplace as companies innovate and develop new products using consumer data, and provide better assurance to consumers that their privacy will be protected.

House Energy and Commerce Committee Chairman Frank Pallone Jr (D-NJ) requested the report from GAO "to examine issues related to federal oversight of Internet privacy," particularly with regard to the authority of the FTC and FCC. Given that Pallone requested the report, it is conceivable that the findings could form the basis of federal privacy legislation considered by his committee. His view, as well as other key committee members, may be revealed later this month at a rumored February 26 hearing to be held by the Consumer Protection and Commerce Subcommittee chaired by Representative Jan Schakowsky (D-IL). It will also be of interest to see how this GAO report is received at the February 27 Senate Commerce, Science, and Transportation Committee hearing titled "Policy Principles for a Federal Data Privacy Framework in the United States." However, it is noteworthy that the GAO did not examine how consumer privacy is currently being regulated under the Health Insurance Portability and Accountability Act regulations or Gramm-Leach-Bliley regulations, perhaps suggesting Pallone is looking to avoid revamping how those industries are regulated and also avoiding possible jurisdictional fights in getting legislation enacted.

Trump EO on AI/DOD Strategy

The Administration released an executive order titled "Maintaining American Leadership in Artificial Intelligence (AI)" and the Department of Defense (DOD) released a detailed summary of the "2018 Department of Defense Artificial Intelligence Strategy." In addition to not releasing the DOD's AI strategy, the Administration also did not release a policy directive referenced in the EO: National Security Presidential Memorandum of February 11, 2019 (Protecting the United States Advantage in Artificial Intelligence and Related Critical Technologies). It is unclear when this document might be released and what it might require of federal agencies.

In the EO, President Donald Trump declared "[i]t is the policy of the United States Government to sustain and enhance the scientific, technological, and economic leadership position of the United States in AI research and development (R&D) and deployment through a coordinated Federal Government strategy, the American AI Initiative (Initiative)." The EO states that "[t]he Initiative shall be coordinated through the National Science and Technology Council (NSTC) Select Committee on Artificial Intelligence (Select Committee)…[and] [a]ctions shall be implemented by agencies that conduct foundational AI R&D, develop and deploy applications of AI technologies, provide educational grants, and regulate and provide guidance for applications of AI technologies, as determined by the co-chairs of the NSTC Select Committee (implementing agencies)." Agencies that fund or direct R&D must prioritize AI funding and projects to the extent possible for the current fiscal year and in formulating their FY 2020 budget requests.

The American AI Initiative will be founded on five principles:

(a) The United States must drive technological breakthroughs in AI across the Federal Government, industry, and academia in order to promote scientific discovery, economic competitiveness, and national security.

(b) The United States must drive development of appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies in order to enable the creation of new AI-related industries and the adoption of AI by today's industries.

(c) The United States must train current and future generations of American workers with the skills to develop and apply AI technologies to prepare them for today's economy and jobs of the future.

(d) The United States must foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application in order to fully realize the potential of AI technologies for the American people.

(e) The United States must promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations.

The EO details an extensive list of AI-related deliverables, including:

- The Departments of Defense, Commerce, Health and Human Services, and Energy, the Administrator of the National Aeronautics and Space Administration, and the Director of the National Science Foundation must "prioritize the allocation of high-performance computing resources for AI-related applications through…increased assignment of discretionary allocation of resources and resource reserves."
- Within six months, the Select Committee, in coordination with the General Services Administration (GSA), must "submit a report to the President making recommendations on better enabling the use of cloud computing resources for federally funded AI R&D."

- Within three months, the Office of Management and Budget (OMB) "shall publish a notice in the *Federal Register* inviting the public to identify additional requests for access or quality improvements for Federal data and models that would improve AI R&D and testing."
- Within six months, "and in accordance with the implementation of the Cross-Agency Priority Goal: Leveraging Federal Data as a Strategic Asset, from the March 2018 President's Management Agenda, agencies shall consider methods of improving the quality, usability, and appropriate access to priority data identified by the AI research community. Agencies shall also identify any associated resource implications."
- Within six months, OMB and other White House offices are required to issue a memorandum to all agencies that shall:
    - inform the development of regulatory and nonregulatory approaches by such agencies regarding technologies and industrial sectors that are either empowered or enabled by AI, and that advance American innovation while upholding civil liberties, privacy, and American values; and
    - consider ways to reduce barriers to the use of AI technologies in order to promote their innovative application while protecting civil liberties, privacy, American values, and United States economic and national security.
- Within six months of issuance of the OMB memorandum, "the heads of implementing agencies that also have regulatory authorities shall review their authorities relevant to applications of AI and shall submit to OMB plans to achieve consistency with the memorandum."
- Within six months, "the National Institute of Standards and Technology (NIST), shall issue a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies."
- Within 90 days of the date of this order, the Select Committee shall provide recommendations to the NSTC Committee on STEM Education regarding AI-related educational and workforce development considerations that focus on American citizens.
- Within 120 days, "the Assistant to the President for National Security Affairs, in coordination with the Office of Science and Technology Policy (OSTP) Director and the recipients of the NSPM, shall organize the development of an action plan to protect the United States advantage in AI and AI technology critical to United States economic and national security interests against strategic competitors and adversarial nations."

The EO appears to pull together existing policy directives and adds new directives to federal agencies to advance AI. In May 2018, the White House released "Summary Of The 2018 White House Summit On Artificial Intelligence For American Industry" which identified a number of the same principles the EO uses to undergird the Administration's new initiative. In mid 2018, OSTP and OMB released the Administration's FY 2020 research and development budget priorities that "provides guidance to agencies as they formulate their Fiscal Year 2020 budget submissions… [and] also details priority practices to effectively leverage R&D resources, including R&D workforce and infrastructure." This directive to agencies on how to order their budget requests prioritized AI. Also, the FY 2019 budget request highlighted AI funding and programmatic requests. The EO builds on these directives with respect to AI and is more directive to agencies as to how to utilize their budgetary resources to achieve the goals of the EO. However, by this point in the FY 2020 budget process, the budget requests of agencies are essentially finalized, meaning agencies would not be able to significantly revise their requests in order to increase funding for AI. Yet, because agencies had been directed to dedicate some resources to AI in these budget requests, there is likely some funding or programmatic language in the requests set to be submitted to Congress next month.

Similarly, the recently enacted "Foundations for Evidence-Based Policymaking Act of 2017" (P.L. 115-435) would require agencies to place a greater emphasis on evidence in policymaking through a variety of means. This bill includes language that would push federal agencies to make more federal data available to the private sector and academia with the goal. Consequently, language in the EO dovetails with the dictates of the statute. Likewise, the President's Management Agenda, particularly its Data Strategy, has already set the Administration on a path to sharing more data. The Administration is still developing its Data Strategy but final principles and draft practices have been released ahead of the issuance of the full strategy.

In September 2018, the Defense Advanced Research Projects Agency (DARPA) announced that it would make "a multi-year investment of more than $2 billion in new and existing programs called the "AI Next" campaign," which includes "automating critical DoD business processes, such as security clearance vetting or accrediting software systems for operational deployment; improving the robustness and reliability of AI systems; enhancing the security and resiliency of machine learning and AI technologies; reducing power, data, and performance inefficiencies; and pioneering the next generation of AI algorithms and applications, such as "explainability" and common sense reasoning." DARPA added that "[i]n addition to new and existing DARPA research, a key component of the campaign will be DARPA's Artificial Intelligence Exploration (AIE) program, which was first announced in July 2018."

Congress has also acted with respect to AI. The FY 2019 National Defense Authorization Act (NDAA) (P.L. 115-232) created a National Security Commission on Artificial Intelligence that "shall consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies by the United States to comprehensively address the national security and defense needs of the United States." Within six months of enactment (mid-March 2019), this commission must "submit to the President and Congress an initial report on the findings of the Commission and such recommendations that the Commission may have for action by the executive branch and Congress related to artificial intelligence, machine learning, and associated technologies, including recommendations to more effectively organize the Federal Government." Members have been named to the commission but a report has not yet been issued.

In the DOD AI Strategy, the Pentagon stated that it "will drive the urgency, scale, and unity of effort needed to navigate this transformation…[and] [t]he Joint Artificial Intelligence Center (JAIC) is the focal point for carrying it out."

The DOD explained that

> Other nations, particularly China and Russia, are making significant investments in AI for military purposes, including in applications that raise questions regarding international norms and human rights. These investments threaten to erode our technological and operational advantages and destabilize the free and open international order. The United States, together with its allies and partners, must adopt AI to maintain its strategic position, prevail on future battlefields, and safeguard this order. We will also seek to develop and use AI technologies in ways that advance security, peace, and stability in the long run. We will lead in the responsible use and development of AI by articulating our vision and guiding principles for using AI in a lawful and ethical manner.

The DOD stated that JAIC will "accelerate the delivery of AI-enabled capabilities, scale the Department-wide impact of AI, and synchronize DOD AI activities to expand Joint Force advantages…[and] the JAIC will:

- Rapidly deliver AI-enabled capabilities to address key missions, strengthening current military advantages and enhancing future AI research and development efforts with mission needs, operational outcomes, user feedback, and data;
- Establish a common foundation for scaling AI's impact across DOD, leading strategic data acquisition and introducing unified data stores, reusable tools, frameworks and standards, and cloud and edge services;
- Facilitate AI planning, policy, governance, ethics, safety, cybersecurity, and multilateral coordination;
- Attract and cultivate a world-class AI team to supply trusted subject matter expertise on AI capability delivery and to create new accelerated learning experiences in AI across DOD at all levels of professional education and training.

In June 2018, Deputy Secretary of Defense Patrick Shanahan issued a memorandum creating the JAIC "with the overarching goal of accelerating delivery of AI-enabled capabilities, scaling the Department-wide impact of AI, and synchronizing DOD AI activities to expand Joint Force advantages." In May 2018, former Secretary of Defense James Mattis sent the President a memorandum arguing that the U.S. needs a national AI strategy.

A 2018 report commissioned by the U.S.-China Economic and Security Review Commission asserted the following:

- **Policy Prioritization:** The Made in China 2025 and Next Generation Artificial Intelligence Plan policies provide two examples of top-down guidance and, most importantly, investment in key technologies. They also signal China's intent to become a global leader in artificial intelligence by 2030 and to build increasingly advanced abilities in other Fourth Industrial Revolution capability areas over the next thirty years. As one professor at Zheijang University's College of Computer Science told *Forbes* magazine, "China is devoting a lot of strength, a lot of determination and a lot of money to AI."
- **China's Investment in the United States High-Tech Sector:** Chinese firms have spent some of this money referred to above to invest in U.S. AI start-ups in order to avoid scrutiny from the Committee on Foreign Investment in the United States (CFIUS), which does not currently cover joint ventures, minority stakes and early-stage investments. Chinese companies have reportedly invested $700 million across 51 U.S. AI companies with some of these companies having links to the U.S. military and other adjacent and strategically important government organizations.
- **China versus the U.S.:** The U.S. currently retains overall global leadership in artificial intelligence, especially in core concepts. However, the velocity of China's progress and alignment of its many levers for further artificial intelligence advancement suggest this advantage will be challenged, first in specific applications of artificial core concepts and then in the game-changing core concepts themselves.

Despite growing concern from government policymakers and some private sector stakeholders, some members of academia see the threat posed by China as not so dire. A 2018 University of Oxford report found that China's AI capabilities "are about half of those of America." The Center for a New American Security argued in a February 2019 report that

> If the United States wants to lead the world in AI, it will require funding, focus, and a willingness among U.S. policymakers to drive large-scale necessary change. U.S. leaders have more powerful tools to influence the technological

and economic competitiveness of the United States than they have tools to influence China's competitiveness. They should prioritize accordingly.

Senate Homeland Security Moves Targeted Cyber Bills

Last week, the Senate Homeland Security Committee marked up and reported out a trio of bills:

- The "National Cybersecurity Preparedness Consortium Act of 2019" (S. 333) would allow the Department of Homeland Security to "work with a consortium to support efforts to address cybersecurity risks and incidents." Consortiums are defined to be "a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security."
- The "Federal Rotational Cyber Workforce Program Act of 2019" (S. 406), which would establish a program under which cybersecurity employees would rotate at federal agencies.
- The "DHS Cyber Hunt and Incident Response Teams Act of 2019" (S. 315), after adopting a substitute amendment, which would require the National Cybersecurity and Communications Integration Center (NCCIC) to "maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents."

Senate Banking Asks Stakeholders For Input On Data Security Legislation

On February 13, Senate Banking Committee Chairman Mike Crapo (R-ID) and Ranking Member Sherrod Brown (D-OH) requested "feedback from interested stakeholders on the collection, use and protection of sensitive information by financial regulators and private companies." Responses are welcome until March 15, 2019, should be submitted to submissions@banking.senate.gov, and "will be made public on the Banking Committee's website." Crapo and Brown stated:

> The collection, use and protection of personally identifiable information and other sensitive information by financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) is something that deserves close scrutiny. Americans are rightly concerned about how their data is collected and used, and how such data is secured and protected. The collection and use of personally identifiable information will be a major focus of the Banking Committee moving forward.

However, the quotes from Crapo and Brown in the joint press release suggest they may not be entirely aligned on the scope of potential privacy legislation. Crapo asserted "it is worth examining how the Fair Credit Reporting Act should work in a digital economy, and whether certain data brokers and other firms serve a function similar to the original consumer reporting agencies." However, Brown remarked that "[i]n the year and a half since the Equifax breach, the country has learned that financial and technology companies are collecting huge stockpiles of sensitive personal data, but fail over and over to protect Americans' privacy." Brown added that "Congress should make it easy for consumers to find out who is collecting personal information about them, and give consumers power over how that data is used, stored and distributed."

Crapo and Brown posed the following questions to stakeholders:

1) What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?
2) What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?
3) What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?
4) What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?
5) What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

House Holds Hearing on Election Security

On February 13, the House Homeland Security Committee held a hearing titled "Defending Our Democracy: Building Partnerships to Protect America's Elections" and focused on the "For the People Act of 2019" (H.R. 1), the House Democrats' election reform package that would, among other policy goals, seek to strengthen state and local governments' cybersecurity posture in the wake of the 2016 election.

The day of the hearing, the online publication *The Daily Beast* ran an article based on information from "three current and former Department of Homeland Security officials" alleging that two task forces dedicated to fighting foreign interference in the 2020 election "are being dramatically downsized." "[A] DHS official familiar with the teams" claimed that "[w]e know Russia is going to be engaged." This official added that "[o]ther state actors have seen the success of Russia and realize the value of disinformation operations…[s]o it's very curious why the task forces were demoted in the bureaucracy and the leadership has not committed resources to prepare for the 2020 election."

This hearing also occurred the same week the Organization for Security and Co-operation in Europe (OSCE) released its final report on the U.S. mid-term elections. The OSCE found that

> large parts of the US election infrastructure remain unprotected and vulnerable and do not provide mechanisms of accountability. This includes, for example, insecure voter registration systems in use in several states, the use of wirelessly networked laptop computers by polling station staff to identify voters, the use of digital media to transfer critical information to and from vulnerable voting machines, or election officials who are, often in cooperation with vendors, not adequately trained for configuring voting machines. Unprepared jurisdictions lack basic cyber-defense capabilities and the capacity to undertake comprehensive feasibility studies that include clear procurement and maintenance plans.

Chairman Bennie Thompson (D-MS) remarked that in February 2018 a joint Task Force on election security of Democrats on the committee and the House Administration Committee produced recommendations and legislation. He stated that the "legislation is now part of H.R. 1, the For the People Act, which the House is expected to consider in the coming weeks." Thompson said that "[t]he Department of Homeland Security (DHS) and Election Assistance Commission (EAC) have built stronger, more effective partnerships with State and local election officials…[b]ut it is unclear whether either agency has the resources necessary to meet the increasing demand for their resources." Thompson stated that "[a]lthough some dispute that the election infrastructure local election officials oversee is vulnerable to hacking, cybersecurity experts have made a credible case it is."

Ranking Member Mike Rogers (R-AL) remarked that the hearings would focus on the work that needs to be done on voting technology and systems. He said that policymakers must keep in mind one central fact: international and domestic hackers and vandals will not follow the law. Rogers pointed to "liberal activists" spreading disinformation during the 2017 Senate race in Alabama. He said H.R. 1 attempts to deal with these problems but the language in the bill is "deeply naïve." Rogers claimed that the bill is "an exercise in regulating everything that moves near a ballot box." He called for a deliberative, bipartisan process to craft an election security bill and decried the bill as a partisan political exercise.

Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs stated that "[w]hile there was activity targeting our election infrastructure leading up to the midterms, this activity is similar to what we have seen previously and occurs on the Internet every day." He stated that "[t]his activity has not been attributed to nation-state actors and along with the Department of Justice (DOJ), we concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections." Krebs stated that "DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continued incentivizing the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the states to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure." He said that "[w]e will also continue to engage any political entity that wants our help…[and] DHS offers these entities the same tools and resources that we offer to state and local election officials, including trainings, cyber hygiene support, information sharing, and other resources."

Election Assistance Commission (EAC) Chair Thomas Hicks stated that "[d]uring the last Presidential Election cycle, the EAC was a key player in federal efforts to share vital security information with the states and educate our federal partners about ways to best serve the needs of election administrators." He stated that "[f]or example, the EAC:

- Distributed urgent security alerts and threat indicators from the DHS and the Federal Bureau of Investigation (FBI) to states and territories to help protect election systems from specific cybersecurity threats.
- Met on multiple occasions with staff from the DHS, the FBI, and the White House to discuss specific and nonspecific threats, state and local election system security and protocols, and the dynamics of the election system and its 8,000 plus jurisdictions nationwide.
- Served as the federal government's primary communication channel to provide real-time cybersecurity information to election officials around the country. This information included current data on cyber threats, tactics for protecting election systems against these threats, and the availability and value of DHS resources for protecting cyber-assets.

- Participated in and convened conference calls with federal officials, Secretaries of State and other State Chief Election Officials, local election administration officials, federal law enforcement, and federal agency personnel to discuss the prospect of designating elections as part of the nation's critical infrastructure. These discussions focused on topics such as coordinating security flashes from the FBI, the implications of a critical infrastructure designation, education on the nation's election system, and the dynamics of successfully communicating information to every level of election officials responsible for running the nation's election system.
- Provided DHS with perspective, information, and data related to the election system, introductions to officials in the election community, and information that assisted the agency with shaping communications in a manner that would be useful to the states and local election officials.
- Published a white paper entitled "U.S. Election Systems as Critical Infrastructure" that provided a basic understanding of critical infrastructure for election officials.
- Contributed to multiple foundational DHS documents used to structure the Elections Systems Critical Infrastructure designation and sector.

Senate Energy Committee Looks At Cybersecurity In Energy Sector

On February 14, the Senate Energy and Natural Resources Committee held a hearing "to consider the status and outlook for cybersecurity efforts in the energy industry."

Chairman Lisa Murkowski (R-AK) stated that "[w]e know that the threat of cyber attacks by our foreign adversaries and other sophisticated entities is real and growing…[and] [l]ast month's 2019 Worldwide Threat Assessment detailed how China, Russia and other foreign adversaries are using cyber operations to target our military and our critical infrastructure." Murkowski stated that "[t]he assessment notes that our electric grid and natural gas pipelines are particularly vulnerable to attack and that Russia is mapping our infrastructure with the long- term goal of causing substantial damage." She said that "[w]e know we don't want that to happen here…[and] [w]e cannot let it happen in the United States." Murkowski said that "[o]ur grid system is 'uniquely critical' and the consequences of a successful cyber-incursion would be widespread and potentially devastating…[and] [t]he resulting loss of power would impact hospitals, banks, cell phone service, gas pumps, traffic lights." She asserted that "[t]he government's focus on cybersecurity, in partnership with industry, is a major reason that the United States has not experienced an attack like Ukraine's."

Ranking Member Joe Manchin (D-WV) said that "[t]his hearing is particularly timely because just a few weeks ago our Director of National Intelligence, Dan Coats, publicly warned of two potential energy cybersecurity attack scenarios: a Russian cyber attack that could disrupt an electrical network for a few hours, and a Chinese cyber attack that could disrupt a natural gas pipeline for weeks." He said that "[t]hese threats are not just theoretical: we know that in 2015 and 2016, Ukraine suffered two devastating power outages as a result of cyber attacks…[a]nd according to the *New York Times*, a petrochemical plant in Saudi Arabia was hit with an even more serious type of cyber attack in 2017." Manchin said that "[e]nergy cybersecurity is national security." He stated that "supply chain security has emerged as a significant focus." Manchin said that "[w]e have to make sure the companies that build components for our grid are secure…[and] [w]e have to protect against vendors' remote access of the grid being exploited, and we have to make sure that attackers don't insert malware into a vendor software update."

Assistant Secretary of Energy for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Karen S. Evans stated that "[o]ur Nation's energy infrastructure has become a primary target for hostile cyber actors, both state-sponsored and non-state sponsored." She asserted that "[t]he frequency, scale, and sophistication of cyber threats have increased…[and] [c]yber incidents have the potential to disrupt energy services, damage highly specialized equipment, and even threaten human health and safety." Evans stated that "[t]he Director of National Intelligence, along with several heads of the Administration's Intelligence Community agencies, recently stated in written testimony that 'China has the ability to launch cyberattacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks.'" Evans said that "Russia has similar abilities with the capability to disrupt 'an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016.'"

Federal Energy Regulatory Commission (FERC) Chairman Neil Chatterjee remarked that "[a]s I discussed in a joint op-ed with my colleague Commissioner Glick last year, I am concerned that, because of our nation's growing use of natural gas for power generation, a successful cyber-attack on the natural gas pipeline system could have a significant impact on the electric grid." He said that "[g]iven this increasing vulnerability, Commissioner Glick and I expressed our view that more must be done to ensure robust oversight for natural gas pipeline cybersecurity." Chatterjee said that "[s]ince the publication of that op-ed, I've been pleased to hear from many members of the natural gas pipeline community who have expressed their appreciation for these concerns and willingness to continue taking steps to improve their security posture." He said that "[i]n addition, I recently met with Transportation Security Administration (TSA) Administrator David Pekoske to discuss pipeline cybersecurity and was impressed by his focus on this vital issue as well as his pledge to taking further action to improve TSA's oversight of pipeline security." Chatterjee said that "[w]hile I think both industry and government have made significant strides toward addressing this issue, I believe more work still needs to be done, and the Commission stands ready to assist in these efforts."

FTC and Facebook Reportedly Negotiating Multi-Billion Dollar Settlement

Last week, the *Washington Post* reported that the Federal Trade Commission (FTC) and social media giant Facebook could be close to a settlement of the FTC's investigation of Facebook's interactions with Cambridge Analytica. The FTC is likely alleging that Facebook violated the 2012 settlement by allowing Cambridge Analytica access to its users' personal information beyond what these users agreed to share. Facebook agreed in the final order issued by the FTC that it would:

> prior to any sharing of a user's nonpublic user information by Respondent with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:
>
> > A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and
> >
> > B. obtain the user's affirmative express consent.

In 2018, a committee of the United Kingdom's (UK) Parliament alleged in an interim report on disinformation and "fake news" that Cambridge Analytica and associated were granted access to 87 million Facebook users. The Digital, Culture, Media and Sport Committee noted that "if the new Data Protection Act 2018 had been in place when the ICO started its investigation into Facebook, the ICO's Notice of Intent to impose 4% of its annual turnover of $7.87 billion, which would have totalled £315 million." In October 2018, the UK's Information Commissioner's Office (ICO) fined Facebook £500,000 "for serious breaches of data protection law."

In November 2011, the FTC and Facebook agreed on a draft consent order regarding the agency's allegations that Facebook violated Section 5 of the FTC Act through its privacy practices, and the FTC issued a final order in August 2012. The 20-year final order required Facebook "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information." Violations of consent orders can allow the FTC to request that U.S. District Court levy civil fines of more than $16,000 per violation.

The FTC's "Analysis of Proposed Consent Order To Aid Public Comment" laid out the agency's "eight violations of Section 5(a) of the FTC Act, which prohibits deceptive and unfair acts or practices in or affecting commerce, by Facebook:

- Facebook's Deceptive Privacy Settings: Facebook communicated to users that they could restrict certain information they provided on the site to a limited audience, such as "Friends Only." In fact, selecting these categories did not prevent users' information from being shared with Apps that their Friends used.
- Facebook's Deceptive and Unfair December 2009 Privacy Changes: In December 2009, Facebook changed its site so that certain information that users may have designated as private– such as a user's Friend List –was made public, without adequate disclosure to users. This conduct was also unfair to users.
- Facebook's Deception Regarding App Access: Facebook represented to users that whenever they authorized an App, the App would only access the information of the user that it needed to operate. In fact, the App could access nearly all of the user's information, even if unrelated to the App's operations. For example, an App that provided horoscopes for users could access the user's photos or employment information, even though there is no need for a horoscope App to access such information.
- Facebook's Deception Regarding Sharing with Advertisers: Facebook promised users that it would not share their personal information with advertisers; in fact, Facebook did share this information with advertisers when a user clicked on a Facebook ad.
- Facebook's Deception Regarding Its Verified Apps Program: Facebook had a "Verified Apps" program through which it represented that it had certified the security of certain Apps when, in fact, it had not.
- Facebook's Deception Regarding Photo and Video Deletion: Facebook stated to users that, when they deactivate or delete their accounts, their photos and videos would be inaccessible. In fact, Facebook continued to allow access to this content even after a user deactivated or deleted his or her account.
- Safe Harbor: Facebook deceptively stated that it complied with the U.S.-EU Safe Harbor Framework, a mechanism by which U.S. companies may transfer data from the European Union to the United States consistent with European law.

DIA Details Russian and Chinese Cyber Threats in Space

The Defense Intelligence Agency (DIA) released a report titled "2019 Challenges to Security in Space" in which the agency observed that "[s]pace-based capabilities provide integral support to military, commercial, and civilian applications." The DIA stated that "China and Russia, in particular, have taken steps to challenge the United States:

- Chinese and Russian military doctrines indicate that they view space as important to modern warfare and view counterspace capabilities as a means to reduce U.S. and allied military effectiveness. Both reorganized their militaries in 2015, emphasizing the importance of space operations.
- Both have developed robust and capable space services, including space-based intelligence, surveillance, and reconnaissance. Moreover, they are making improvements to existing systems, including space launch vehicles and satellite navigation constellations. These capabilities provide their militaries with the ability to command and control their forces worldwide and also with enhanced situational awareness, enabling them to monitor, track, and target U.S. and allied forces.
- Chinese and Russian space surveillance networks are capable of searching, tracking, and characterizing satellites in all earth orbits. This capability supports both space operations and counterspace systems.
- Both states are developing jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and ground-based antisatellite missiles that can achieve a range of reversible to nonreversible effects.

Regarding "Cyberspace Threats," the DIA provided the following assessments:

- China emphasizes offensive cyberspace capabilities as key assets for integrated warfare and could use its cyberwarfare capabilities to support military operations against space-based assets. For example, the People's Liberation Army (PLA) could employ its cyberattack capabilities to establish information dominance in the early stages of a conflict to constrain an adversary's actions, or slow its mobilization and deployment by targeting network-based command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), logistics, and commercial activities. The PLA also plays a role in cyberespionage targeting foreign space entities, consistent with broader state-sponsored industrial and technical espionage to increase the level of technologies and expertise available to support military research and development and acquisition. The PLA unit responsible for conducting signals intelligence has supported cyberespionage against U.S. and European satellite and aerospace industries since at least 2007.
- Since at least 2010, the Russian military has prioritized the development of forces and capabilities, including cyberspace operations, for what it terms "information confrontation," which is a holistic concept for ensuring information superiority. The weaponization of information is a key aspect of this strategy and is employed in times of peace, crisis, and war. Russia considers the information sphere to be strategically decisive and has taken steps to modernize its military's information attack and defense organizations and capabilities.

Other Hearings and Events

"For the People: Our American Democracy" – House Administration

Further Reading

"Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security" – Center for a New American Security
"Toward AI Security: Global Aspirations for a More Resilient Future" –Center for Long-Term Cybersecurity
"The American AI Initiative: Bluster or Gangbuster?" – Center for Strategic and International Studies
"EU Considers Response to China Hacking After U.K. Evidence, Sources Say" – Reuters
"U.S. judge keeps documents secret in Facebook encryption case" – Reuters
"Senate committee leaders worry no one's in charge on cybersecurity" – Washington Post
"China's cybersecurity law update lets state agencies 'pen-test' local companies" – ZDNet
"Exploring the Russian Social Media Campaign in Charlottesville" – National Security Archive
"Don't Let Cyber Attribution Debates Tear Apart the NATO Alliance" – Lawfare