Technology Policy Update
21 February 2020
By Michael Kans, Esq.

Trump Administration Budget Calls For Continued Funding For Cybersecurity and R&D

Last week, the Trump Administration released its FY 2021 budget request and even though it is asking that Congress again radically remake the federal civilian budget through deep cuts and eliminating programs it deems wasteful, duplicative, overlapping, or ineffective, there is also an emphasis on a number of technology programs, including cybersecurity, information technology modernization, artificial intelligence, and quantum computing. However, like the last two budget requests, Congress will most likely disregard the requests for funding cuts and will instead enact a modest increase above the current year's enacted funding. The Administration is proposing budget authority of $1.340 trillion for discretionary funding with $741 billion for defense programs (with $69 billion funded through Overseas Contingency Operations accounts) and $600 billion for non-defense. In a footnote to a summary table, the Administration explained it is "propos[ing] to fund base defense programs for 2021 at the existing [Budget Control Act] cap and fund base [non-defense] programs at a level that is five percent below the 2020 [non-defense] cap." The Administration is asking that Congress "extend the [Budget Control Act] caps through 2025 at the levels included in the 2021 Budget…[which] would provide an increase in defense funding of about two percent each year, and decrease funding for [non-defense] programs by two percent (or "2-penny") each year."

In his cover note to the budget request, President Donald Trump stated

> As we enter the 2020's, our Nation confronts new challenges and opportunities. The 21st century requires us to focus on great power rivals; prioritize artificial intelligence, 5G, and industries of the future; and to protect our research and environment from foreign government influence. To meet these challenges and seize these opportunities, we must shift the Government out of its old and outdated ways. This will require each and every Government agency to do more to prepare for the demands of tomorrow.

The White House touted the $18.8 billion that it is requested for cybersecurity programs but noted "[d]ue to the sensitive nature of some activities, this amount does not represent the entire cyber budget." The Administration wants to spend a projected $92 billion on information technology, with "[t]he Department of Homeland Security (DHS) is the largest civilian agency in IT spending, while the bottom five agencies represent 1.1 percent of Federal civilian IT spending." Additionally, the Trump Administration is asking Congress for $142.2 billion in federal research & development (R&D). The Administration emphasized that it "is prioritizing the science and technology that underpin the Industries of the Future (IotF)—artificial intelligence (AI), quantum information science (QIS), 5G/advanced communications, biotechnology, and advanced manufacturing." The White House claimed that "[r]elative to the 2020 President's Budget, this includes major increases in QIS and non-defense AI R&D as part of a commitment to double Federal AI and QIS R&D investments by 2022. R&D investments in AI and QIS, in particular, act as innovation multipliers and employment drivers, not only by promoting science & technology (S&T) progress across many disciplines, but also by helping to build a highly-skilled American workforce."

Of course, the Trump Administration touted certain programmatic initiatives in the budget. In the third chapter of the budget summary ("Countering Emerging Threats,") the Administration highlighted the following as being part of "PROTECTING AMERICA'S ECONOMY:"

- **Defending Government Networks and Critical Infrastructure.** The Department of Homeland Security (DHS) continues to play a major role in securing and building cybersecurity resilience for the Nation's most critical infrastructure, including Government networks. DHS, in partnership with key stakeholders, identifies and manages the most critical national cybersecurity risks. The Budget includes more than $1.1 billion for DHS's cybersecurity efforts.
- **Addresses the Federal Cybersecurity Workforce Shortage.** To face today's threats and prepare for tomorrow's, America must have a workforce that is trained and skilled in cybersecurity. Today, there are simply not enough cyber professionals in Government service. The *Delivering Government Solutions in the 21st Century* plan and executive Order 13870, "America's Cybersecurity Workforce" included several initiatives to solve the Federal cybersecurity workforce shortage, establishing unified cyber workforce capabilities across the civilian enterprise. The Budget includes funding to support DHS's Cyber Talent Management System and for the Cybersecurity and Infrastructure Security Agency, which would lead a Government-wide cybersecurity workforce program for all Federal cyber professionals.

In the "DELIVERING A MORE RESPONSIVE, AGILE, AND EFFICIENT GOVERNMENT," chapter, the Administration highlighted the following:

- **Saves Money with Category Management.** The Federal Government spends over $350 billion on common goods and services every year. Through the category management initiative, the Administration has aggregated demand for common goods and services, leveraged innovative procurement strategies, and improved data analytics. As a result, the Administration has reduced duplicative contracts by 26 percent, increased contract dollars to small businesses, created opportunities for new entrants, avoided costs of $27 billion, and is on track to achieve $36 billion in savings by the end of 2020. The Budget includes resources to further support statutory and regulatory changes to leverage procurement data more strategically and reduce expensive friction in acquisitions.
- **Improves Acquisitions in the Digital Age**. Modernizing the Federal acquisition system for the digital age requires the development of tactical strategies and practical tools that support improved access to business intelligence, as well as the accelerated identification, testing, and adoption of meaningful changes to business practices. To accelerate the pace of modernization, the Administration will baseline the current state of acquisition innovation, pilot a centralized information sharing knowledge management resource, promote emerging technologies, and scale application of a proven model to coach innovative practices.
- **Leverages Data as a Strategic Asset**. The world is creating data faster than ever before, with 90 percent of the data on the Internet created since 2016. Data from Federal programs should be used as a strategic asset to grow the economy, facilitate oversight, and promote transparency. After a year and a half of work and input from hundreds of stakeholders, the Administration released the *Federal Data Strategy 2020 Action Plan*, a significant milestone in the effort to create a coordinated approach to Federal data use and management that serves the public.
- **Addresses the Federal Cybersecurity Shortage**. A cyber reskilling pilot program offers Federal employees the opportunity for hands-on training in cybersecurity, one of the fastest

growing fields in the Nation and critical to protecting Government data from bad actors. These projects demonstrate a path forward for reskilling Federal employees to achieve and sustain needed skills inside the Federal workforce.

- **Secures the National Supply Chain**. In 2019, as part of the National Cyber Strategy and the SECURE Technology Act, agencies were required to assess the risks to their respective in- formation and communications technology supply chains. The Administration established the Federal Acquisition Security Council to help agencies safeguard information and communication technology from emerging threats and support the need to establish standards for the acquisition community with respect to supply chain risk management.
- **Improves Management of Acquisitions**. In 2019, the Administration took steps to establish an official career path for program managers to ensure they are appropriately trained and certified to collaborate with contracting officials in managing major acquisitions. Agencies also created and strengthened structures to manage similar investments in their portfolios and identified priority projects for heightened management attention.

In the summary for the Department of Defense (DOD), the Administration also emphasized the following programs in the "***Funds Leading Edge Innovation***" section*:*

- **Ensures Technological Superiority by Investing in Industries of the Future.** The Budget supports critical investments to regain and sustain U.S. technological superiority to counter and overmatch emerging threats. The Budget invests over $14 billion in DOD science and technology programs that support key investments in industries of the future, such as artificial intelligence, quantum information science, and biotechnology, as well as core DOD modernization priorities such as hypersonic weapons, directed energy, 5G, space, autonomy, microelectronics, cybersecurity, and fully-networked command, control, and communications.
- **Ensures Access to Trusted and Assured Microelectronics.** The Budget invests in necessary enhancements to ensure that the United States can maintain trusted and reliable access to state- of-the-art microelectronics suppliers. The Budget enables secure design, development, fabrication, and assembly of microelectronics without the need to invest in a costly Government-owned and operated fabrication facility. These investments are essential for the development of next generation capabilities in communications, computing, artificial intelligence, and autonomy.
- **Invests in Cyber Capability.** The Budget builds on progress in recent years to develop the military's cyber capabilities by requesting nearly $10 billion in 2021. The cyber budget is aligned to advance DOD's three primary cyber missions: safeguarding DOD's networks, information, and systems; supporting military commander objectives; and defending the Nation. This investment provides the resources necessary to grow the capacity of U.S. military cyber forces, including U.S. Cyber Command, invest in the cyber workforce, and continue to maintain the highest cybersecurity standards at DOD.

The Administration also highlighted potential savings: ***Promotes Reform, Efficiency, and Accountability***

- **Achieves Savings across the Department.** The Budget reflects the Administration's commitment to ensuring good stewardship of taxpayer dollars by prioritizing resources for lethality and readiness initiatives. The Budget supports the Department's comprehensive review of DOD's Fourth estate to ensure alignment with the National Defense Strategy and free up time, money, and manpower to reinvest in the Department's highest priorities. As part of this effort, known as the Defense-Wide review, DOD identified over $5 billion in savings in 2021 to reallocate toward higher strategic priorities. The review also transferred

> an additional $2 billion in activities and functions to the military departments for more effective and efficient operations. The Budget reduces most DOD offices outside the military departments by at least five percent in an effort to counter defense-wide programs' growing share of the total DOD budget. The effort seeks to restore the appropriate balance between defense-wide organizations and the military departments, while promoting long-term structural reform of DOD's defense-wide activities.

In the DOD's Overview of the FY 2021 budget request, the Pentagon offered the following overview of cyber activities:

CYBERSPACE ACTIVITIES

The Department Cyber Strategy identifies five cyberspace objectives that must be met to implement the NDS:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace domain.
2. Enhancing Joint Force military advantages through the integration of cyber capabilities into planning and operations.
3. Deterring, preempting, or defeating malicious cyber activity targeting U.S. critical infrastructure that is likely to cause a significant cyber incident.
4. Securing DOD information and systems, including on non-DOD-owned networks, against cyber espionage and malicious cyber activity.
5. Expanding DOD cyber cooperation with allies, partners, and private sector entities.

The FY 2021 Cyberspace Activities budget ($9.8 billion) continues to build on the goals laid out in the Digital Modernization Strategy (DMS); Innovate for Competitive Advantage, Optimize for Efficiencies and Improve Capability, Evolve Cybersecurity for Agile and Resilient Defense Posture, and Cultivate Talent for a Ready Digital Force. The budget has been optimized to support the implementation of the Cyber Strategy by funding programs and activities that advance cybersecurity, cyberspace operations, and advanced cyber research and development activities:

A. The $5.4 billion Cybersecurity budget for FY 2021 builds on the important initiatives established in FY 2020 and provides for increased capabilities in Cross Domain Solutions, Next-Generation Encryption Solutions, and Network Modernizations.

B. The FY 2021 Cyber Operations budget ($3.8 billion) supports the implementation of the Cyber Strategy by funding programs and activities that advance:

   - Cooperation with allies and partners in the conduct of "hunt forward" defensive cyberspace operations to counter malign cyber actors (FY 2021, $431.6 million)
   - The development of capabilities to integrate joint, coalition and inter-agency command and control to enhance multi-domain operations (FY 2021, $238.6 million)
   - DOD mission assurance activities that allow the Department to better understand the risks to its key missions and to increase resilience and implement mitigations to reduce the vulnerability of key assets (FY 2021, $460.4 million)

   The Cyber Operations budget includes $2.2 billion to continue support for Cyber Mission Forces (CMF).

C. The FY 2021 Cyberspace Activities budget includes resources for advanced cyber related research and development activities ($0.6billion).

Regarding the Department of Homeland Security's (DHS) cyber mission, the Administration offered the following:

- **Addresses the Cybersecurity Workforce Shortage.** The *Delivering Government Solutions in the 21st Century* plan and executive Order 13870, "America's Cybersecurity Workforce," included several initiatives to solve the Federal cybersecurity workforce shortage by establishing unified cyber workforce capabilities across the civilian enterprise. The Budget includes funding to support DHS's Cyber Talent Management System, which reflects the exemption of DHS's cyber workforce from many of the hiring and compensation requirements and restrictions in existing law under title 5 of the United States Code. The Budget also includes additional funding for the Cybersecurity and Infrastructure Security Agency (CISA) to lead a Government-wide cybersecurity workforce program for all Federal cyber professionals, including an interagency cyber rotational program, a cybersecurity training program for all Federal cyber professionals, and a cyber-reskilling academy. CISA will also spearhead the President's Cup Competition, as described in executive Order 13870.
- **Supports Network and Critical Infrastructure Security.** The Department continues to play a major role in securing and building cybersecurity resilience for the Nation's most critical infrastructure, including Government networks. In partnership with key stakeholders, DHS identifies and manages the most critical national cybersecurity risks. The Budget includes more than $1.1 billion for DHS's cybersecurity efforts. These resources would increase the number of DHS-led network risk assessments from 1,800 to more than 6,500—including assessments of State and local electoral systems. The Budget also supports additional tools and services, such as the EINSTEIN and the Continuous Diagnostics and Mitigation programs, to reduce the cybersecurity risk to Federal information technology networks.

However, DHS is proposing a budget cut for the Cybersecurity and Infrastructure Security Agency (CISA) from its current level of funding of $2.015 billion in FY 2020 to $1.758 billion in FY 2021. In its Congressional Budget Justification for the CISA, DHS stated its budget request for CISA "provides $1.8 billion in discretionary funds, including:

- $1.1 billion for cybersecurity efforts to protect the Federal ".gov" domain of civilian networks and partner with the private sector to increase the security of critical networks;
- $96.1 million for infrastructure security efforts to secure and increase resilience for critical infrastructure against all hazards through risk management and collaboration with the critical infrastructure community;
- $157.6 million to ensure emergency communication interoperability and provide assistance and support to Federal, State, local, tribal, territorial stakeholders;
- $166.7 million for Integrated Operations for CISA's frontline, externally-facing activities to ensure seamless support and expedited response to critical needs;
- $91.5 million for the National Risk Management Center to provide infrastructure consequence analysis, decision support, and modeling capabilities to public and private sector partners;
- $37.5 million for Stakeholder Engagement and Requirements to foster collaboration, coordination, and a culture of shared responsibility for national critical infrastructure risk management and resilience with Federal, State, local, tribal, territorial, and private sector partners within the United States, as well as with our international partners abroad;•$141.1M for mission support activities.

DHS touted "[a]dditional highlights:

- $370.1 million for the National Cybersecurity Protection System/EINSTEIN, an integrated system-of-systems that delivers a range of capabilities, including intrusion detection, analytics, intrusion prevention, and information sharing capabilities, that defend the civilian Federal Government's information technology infrastructure from cyber threats.

- $281.7 million for the Continuous Diagnostics and Mitigation to fortify the cybersecurity of government networks and systems."

Democrat Proposes Creating Data Protection Authority To Address Privacy

Another Senate Democrat has introduced a privacy and data security bill. Senator Kirsten Gillibrand's "Data Protection Act of 2020" (S. 3300) would create a federal data protection authority along the lines of the agencies each European Union member nation has. This new agency would be the primary federal regulator of privacy laws, including a number of existing laws that govern the privacy practices of the financial services industries, healthcare industry, and others. This new agency would displace the Federal Trade Commission (FTC) regarding privacy matters but would receive similar enforcement authority but with the ability to levy fines in the first instance. However, state laws would be preempted only if they are contrary to the new regime, and state attorneys general could enforce the new law. A private right of action would not, however, be created under this law.

The bill would establish the Data Protection Agency (DPA), an independent agency headed by a presidentially nominated and Senate confirmed Director who may serve for a five year term normally or more time until a successor is nominated and confirmed. Hence, Directors would not serve at the pleasure of the President and would be independent from the political pressure Cabinet Members may feel from the White House. However, the Director may be removed for "inefficiency, neglect of duty, or malfeasance in office." Generally, the DPA "shall seek to protect individuals' privacy and limit the collection, disclosure, processing and misuse of individuals' personal data by covered entities, and is authorized to exercise its authorities under this Act for such purposes."

Personal data is defined widely as "any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or device" including a number of different enumerated types of data such as medical information, biometric information, browsing history, geolocation data, political information, photographs and videos not password protected, and others. The bill also creates a term "high-risk data practice" to cover the collection of processing of personal data that is sensitive, novel, or may have adverse, discriminatory real world effects and would be subject to heightened scrutiny and regulation. For example, new high-risk data practices "or related profiling techniques" may not be used before the DPA conducts "a formal public rulemaking process," which under administrative law is usually meant as a lengthy process including a public hearing.

Those entities covered by the bill are "any person that collects, processes, or otherwise obtains personal data with the exception of an individual processing personal data in the course of personal or household activity," an incredibly broad definition that sweeps in virtually any commercial entity collecting or processing personal data. There is no carve out for businesses below a certain revenue level or number of persons whose data they collect and process. Large covered entities would be subject to extra scrutiny from the DPA and extra responsibility. Entities falling into category are those with "gross revenues that exceed $25,000,000;" that buy, receive for the covered entity's commercial purposes, sells, or discloses for commercial purposes the personal information of 50,000 or more individuals, households, or devices; or that drive "50 percent or more of its annual revenues from the sale of personal data." The DPA "may require reports and conduct examinations on a periodic basis" from large covered entities to ensure compliance with federal privacy laws, examine their practices, compliance processes, and procedures, "detecting and assessing associated risks to individuals and groups of individuals;" and "requiring and overseeing ex-ante impact assessments and ex-post outcome audits of high-risk data practices to advance fair and just data practices."

Most notably, it appears that the enforcement and rulemaking authority of current privacy statutes would be transferred to the agency, including Title V of the "Financial Services Modernization Act of 1999" (aka Gramm-Leach-Bliley), Subtitle D of the Health Information Technology for Economic and Clinical Health Act (i.e. HIPAA's privacy provisions), the "Children's Online Privacy Protection Act," and the "Fair Credit Reporting Act." Specifically, the bill provides "[t]he Agency is authorized to exercise its authorities under this Act and Federal privacy law to administer, enforce, and otherwise implement the provisions of this Act and Federal privacy law." The bill defines "federal privacy law" to include all the aforementioned statutes. Consequently, the agencies currently enforcing the privacy provisions of those statutes and related regulations would turn over enforcement authority to the DPA. This, of course, is not without precedent. Dodd-Frank required the FTC to relinquish some of its jurisdiction to the Consumer Financial Protection Bureau (CFPB) to cite but one recent example. In any event, this approach sets the "Data Protection Act of 2020" apart from a number of the privacy bills, and aside from the policy elegance of housing privacy statutes and regulations at one agency, this would likely cause the current regulators and the committees that oversee them to oppose this provision of the bill.

The DPA would receive authority to punish unfair and deceptive practices (UDAP) regarding the collection, processing, and use of personal data, but unlike the FTC, notice and comment rulemaking authority to effectuate this authority as needed. However, like the FTC, before the agency may use its UDAP powers regarding unfairness, it must establish the harm would is causing or is likely to cause substantial injury, is unavoidable by the consumer, and is not outweighed by countervailing benefits.

The DPA would receive many of the same authorities the FTC currently has to punish UDAP violations, including injunctions, restitution, disgorgement, damages, and other monetary relief, and also the ability to levy civil fines. However, the fine structure is tiered with reckless and knowingly violations subject to much higher liability. The first tier would expose entities to fines of $5,000 per day the violation is occurring or that the entity fails to heed a DPA order. The language could use clarification as to whether this means per violation per day or just a per day fine regardless of the number of separate violations. Nonetheless, the second tier is for reckless violations and the fines could be as high as $25,000, and the third tier for knowing violations for $1,000,000. However, the DPA must either give notice to entities liable to fines an opportunity and a hearing before levying a fine through its administrative procedures or go to federal court to seek a judgment. However, the DPA could enforce the other federal privacy laws under their terms and not bring to bear the aforementioned authority.

There would be no preemption of state laws to the extent such privacy laws are not inconsistent with the "Data Protection Act of 2020" and states may maintain or institute stronger privacy laws so long as they do not run counter to this statute. This is the structure used under Gramm-Leach-Bliley, and so there is precedence. Hence, it is possible there would be a federal privacy floor that some states like California could regulate above. However, the bill would not change the preemption status quo of the federal privacy laws the DPA will be able to enforce, and those federal statutes that preempt state laws would continue to do so. State attorneys general could bring actions in federal court to enforce this law, but no federal private right of action would be created.

Of course, the only other major privacy and data security bill that would create a new agency to regulate these matters instead of putting the FTC in charge is Representatives Anna Eshoo (D-CA) and Zoe Lofgren's (D-CA) bill, the "Online Privacy Act of 2019" (H.R. 4978) that would create the U.S. Digital Privacy Agency (DPA) that would supersede the FTC on many privacy and data security issues. For many sponsors of privacy bills, creating a new agency may be seen as a few bridges too far, and so they have opted to house new privacy regulation at the FTC.

Finally, as can be seen in her press release, Gillibrand's bill has garnered quite a bit of support from privacy and civil liberties advocates, some of which generally endorses the idea of a U.S. data protection authority and not this bill per se. Nonetheless, this is another bill that is on the field, and it remains to be seen how much Gillibrand will engage on the issue. It also bears note that she serves on none of the committees of jurisdiction in the Senate.

Hearing on State and Local Cybersecurity

Last week, the Senate Homeland Security and Governmental Affairs Committee conducted a hearing to discuss the state of cybersecurity among state, tribal, and local governments in light of the increasing number of ransomware attacks of these jurisdictions in recent years that have sometimes resulted in the loss of data or payment of ransom. The committee was interested in how the Trump Administration, particularly the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), could provide expertise and aid to these governments, and what, if any, legislation Congress should consider. To date, a number of bills gauged to addressing these sorts of problems have been introduced and considered to different degees, including the "State and Local Cybersecurity Improvement Act" (H.R. 5823), the "State and Local Government Cybersecurity Act of 2019" (S. 1846), and the "DOTGOV Online Trust in Government Act of 2019" (S. 2749).

Chair Ron Johnson (R-WI) stated "[t]he protection of mission-critical systems for state, local, tribal, and territorial (SLTT) governments is an essential component of our nation's cybersecurity." He noted that "[l]ast year alone, cybercriminals used ransomware attacks to cripple municipal entities with near impunity…[and] [a]n estimated 966 government, education, and healthcare entities were victims of ransomware attacks in 2019 that cost an estimated $7.5 billion in operational and financial damages." Johnson claimed that "[i]n addition to the increased frequency of ransomware attacks, heightened tensions between the U.S. and Iran have raised concerns about the extent to which state and local governments, and critical infrastructure owners and operators, are prepared to respond to cyberattacks by state or state-sponsored actors." He remarked that "[e]arlier this year, DHS issued multiple alert bulletins referencing potential Iranian cyberattacks against our critical infrastructure in retaliation for the U.S.'s lethal strike against Qassem Soleimani, then head of Iran's Islamic Revolutionary Guard Corps, a designated Foreign Terrorist Organization." He added that "[o]ne bulletin referenced Iran's 'willingness to push the boundaries of their activities, which include destructive wiper malware and, potentially, cyber-enabled kinetic attacks.'"

Johnson said that "[f]ortunately, according to Leidos, a defense, science, and information technology research company, '[a] handful of hygiene measures can stop up to 95 percent of targeted cyber intrusions.'" He contended that "[i]n other words, simple, cost-effective actions can make a tremendous difference…[and] [i]n addition to practicing good cyber hygiene, SLTT governments, and critical infrastructure owners and operators can also leverage DHS resources to help further protect their cybersecurity systems and assets." Johnson stated that "DHS, specifically the Cybersecurity and Critical Infrastructure Security Agency (sic), plays a key role in sharing cyber threat information and cyber hygiene practices." He contended that "[t]he Department also offers assistance to help these entities better protect their mission-critical systems, such as penetration testing, and it also offers recovery assistance if an incident does occur."

Johnson stated that "[s]tate and local governments and the private sector are on the front lines and grappling with these cyber threats every day." He stated that "[f]or example, this past August, Texas was hit by a coordinated ransomware attack…[and] [t]he ransom was not paid, but the response effort still cost the state hundreds of thousands of dollars…[and] DHS assisted in the response through reverse engineering the malware, but according to state officials, additional improvements are needed." Johnson stated that "[w]e can learn a great deal from the experiences of individual states and businesses, and identify areas for improvement."

Ranking Member Gary Peters (D-MI) remarked "[t]he cyber threats facing our nation are becoming increasingly sophisticated and we are all at risk – families, government agencies, schools, small businesses, and critical infrastructure." He stated that "[i]n today's digital world, state and local governments are responsible for safeguarding everything from election systems to sensitive personal data, including social security numbers, credit card information and even medical records." Peters noted that "[s]tate and local governments don't always have the tools to defend against cyber-attacks…[and [f]inancial constraints, workforce challenges, and outdated equipment are all serious challenges for states and cities."

Peters stated that "[a]ttackers always look for the "weakest link" and that's why we must ensure that everyone from small businesses to our state and local governments have the tools to prevent, detect and respond to cyber-attacks…[and] [t]hat's why I have introduced commonsense, bipartisan legislation with my colleagues on this committee to help bolster our cyber security defenses at all levels of government." He said that "I introduced the bipartisan "DOTGOV Act" with Chairman Johnson and Senator [James] Lankford (R-OK) to help state and local governments transition to the more trusted and secure dot-gov domain." Peters added "I also introduced the "State and Local Government Cybersecurity Act" with Senator [Rob] Portman (R-OH)…[which] will help DHS share timely information, deliver training and resources, and provide technical assistance on cybersecurity threats, vulnerabilities, and breaches with states and localities."

Peters stated "[i]n 2016 – in my home state of Michigan, hackers used a ransomware attack on the Lansing Board of Water and Light, forcing taxpayers to pay a $25,000 ransom to unlock the targeted computer systems…[and] [m]y bill would give cities and states the tools to prevent and respond to these kinds of attacks more effectively." He claimed that "[r]ecently, Richmond Community Schools in Michigan were closed for a week due to a similar attack demanding a $10,000 payment…[and] [l]uckily, their data was not compromised." Peters cautioned that "this attack exposes a dangerous vulnerability as schools maintain a considerable amount of sensitive records related to their students and employees – including family records, medical histories, and employment information." He stated that "I introduced the "K-12 Cybersecurity Act of 2019" (S. 3033) with Senator [Tim] Scott (R-SC) to protect students and their data by providing better cybersecurity resources and information to K through 12 schools in Michigan and across the country." Peters declared that "[i]t is clear that these kinds of attacks are only growing and they pose a serious risk…[and] I will continue working to ensure that all of our state and local governments have the resources, information and expertise they need to safeguard Americans."

Regarding his agency's assistance to SLLT governments, CISA Director Christopher C. Krebs stated

> .In July 2019, CISA released a joint statement with our partners at the Multi-State Sharing and Analysis Center, (MS-ISAC), the National Governor's Association (NGA) and the National Association of State Chief Information Officers (NASCIO) with three simple, actionable steps to increase state and local resilience against ransomware. These steps included, Back Up Your System; Reinforce Basic Cybersecurity Awareness and Education; and Revisit and Refine Cyber Incident Response Plans.

Krebs added

In the fall of 2019, CISA released several resources aimed at assisting its stakeholders in raise the level of their cybersecurity practices. These resources include:

- ***CISA Insights - Ransomware Outbreak***: The Insights document focuses on Ransomware and building a better understanding of how attacks are taking place and what actions can be done to mitigate such attacks. The document includes elements like: backing-up data, system images, and configurations and keep the backups offline; updating and patching systems; reviewing and exercising incident response plans; and asking for help from CISA, the FBI, or the Secret Service.
- ***CISA's Cyber Essentials***: The Essentials document is a guide for leaders of small and medium businesses as well as leaders of state, local, tribal and territorial government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
- ***Ransomware Cyber Tabletop Exercise Package:*** Commonly referred to as "exercise in a box," the Exercise Package is as a resource for state, local, and private sector partners that includes template exercise objectives, scenario, and discussion questions, as well as a collection of ransomware and cybersecurity references and resources. Partners can use the exercise package to initiate discussions within their organizations about their ability to address the threat of ransomware, which is impacting the community with increasing frequency.

Krebs added

> At CISA, we believe that there are six key attributes of a successful cyber program. Two strategic attributes are leadership engagement and a culture of security. Two technical attributes are knowing what is on your network and knowing who is on your network. Finally, the two tactical attributes are being able to recover after an incident, utilizing backups that have been tested and having a plan in place that includes outreach to employees, public, etc. CISA actively coordinates with our state and local stakeholders to better understand the support they need to defend their systems from a ransomware attack. CISA utilizes a layered approach to supporting SLTTs through direct assistance, indirect assistance, and self-service capabilities to raise their level of cyber resilience. CISA funds the MS-ISAC, that not only provides a range of free services, but also serves as a network where SLTT agencies can share best practices and lessons learned with each other. Additionally, our partnerships with the private sector are essential. Private sector companies are regularly called in to

> help victims rebuild systems. We need partnerships and input from them as we continue to build out and strengthen our incident efforts.

Texas Department of Information Resources Executive Director Amanda Crawford remarked "[r]ecommendations for improving federal participation include:

- Better sharing of classified information with state government: Currently, our receipt of timely and complete classified information about cyber threats facing our systems is sporadic.
- Increasing DHS-CISA resources per region: Having a dedicated resource to work with the Chief Information Security Officer of each state would help to drive incident response planning and preparedness and would better integrate federal resources into each state.
- Clearly communicating what federal resources are available to state and local governments and how to receive those services: Because these large-scale cyber incidents are a relatively recent development, clear delineations of roles and responsibilities have not
- been sufficiently communicated from the federal government to the state and local level. Multiple federal agencies provide cyber assistance of some sort and it can be challenging and inefficient, particularly in the middle of a cyber event, to know what help is available and who to call. A single federal point of contact who can then coordinate with other potential federal resources would be helpful.
- Balancing the law enforcement need to protect investigations with the ability to share information about active threats: It is critical to be able to share information with the cybersecurity community to prevent the same attack from occurring elsewhere. While we understand law enforcement's goal of catching the criminals responsible for these attacks, the ability to release more specific information would be helpful for the information security community who protects critical assets."

AI Bias Hearing

The House Financial Services Committee's Task Force on Artificial Intelligence held a hearing titled "Equitable Algorithms: Examining Ways to Reduce AI Bias in Financial Services." The memorandum provided by majority committee staff before the hearing explained:

> Applying the existing legal framework where rights and protections are clearly defined to these AI technologies could pose challenges for regulators as they attempt to gauge compliance with many of these laws that do not contemplate the use of AI. In addition, the institutions using the algorithm must be able to explain to regulators: (1) why something happened, (2) why something else did not happen, (3) how failure and success are defined, and (4) how are errors corrected. Presently, these factors translate into regular audits of algorithms for bias and discrimination by regulators or independent third-parties. A similar system is in place in the Europe Union, where its General Data Protection Regulation (GDPR) requires organizations to be able to explain their algorithmic decisions.

Chair Bill Foster (D-IL) said the Task Force is looking to understand what it means to design ethical algorithms that are transparent and fair. He added in short, how do we program fairness into our AI models and make sure they can explain their decisions to us. Foster said there have been a number of recent reports on bias in the lending space from credit cards that discriminate against women to loans that discriminate based on where you went to school. He asserted a lot of the issues are a lot more complicated and nuanced than there are portrayed in the media, but it is clear that the use of AI is hitting a nerve with a lot of folks. He said that for consumers to understand AI, a deeper look is necessary.

Foster noted there are dozens of definitions of fairness, and policymakers should be able to explicitly state what kind of fairness they are looking for and how multiple definitions of fairness are balanced against each other. He contended that while there are laws on equal lending, translating these analogue statutes into machine learning models is easier said than done. He asserted that lawmakers must articulate their goals and then list the tradeoffs that are worth being made between accuracy and fairness. Foster said that it is equally important to ensure ethical algorithms are working as they are intended to. He remarked AI models present novel issues for resource strapped regulators that are not necessarily present in traditional lending models. Foster said that AI models continuously learn from new data, which means that that the models themselves must adapt and change. Foster stated that another challenge is biased data and referenced the saying that life is like a sewer: what one gets out of it depends on what one puts into it. He claimed that AI algorithms are the same and suggested the committee's work may be to define the primary, secondary, and tertiary sewage treatment systems to ensure higher quality output from algorithms.

Foster added that because AI models often rely on historical data, these reflect historical biases, which will ideally disappear over time. He contended that algorithms must, consequently, correct for these biases. Foster asserted that as more data are added to models, there is the possibility that these new data will be used as proxies for characteristics like race will only increase. He said the committee keeps hearing that one potential solution is that algorithms should be audited by expert third parties. He said another idea is for companies to regulate run analyses of their algorithms and then submit the results to regulators for review, which recognizes that building models is an iterative process and there must be the means to respond to these different iterations. Foster stated that the committee wants to ensure that the biases of the analogue world are not recreated in the algorithmic world.

Ranking Member Barry Loudermilk (R-GA) said the committee has discussed algorithms conceptually many times but has not delved into what algorithm explainaibility really means. He stated that analytical models of AI and machine learning are best understood when they are broken into three basic models: 1) descriptive analytics that analyzes past data; 2) predictive analytics which predicts future outcomes based on past data; and 3) prescribing analytics where the algorithm recommends a course of action based on past data. Loudermilk stated there is also a fourth emerging model he refers to as the "execution model" which automatically takes action based on other AI systems' outputs. He stated his belief that the execution model deserves the most attention from policymakers because it can remove the human element in decision-making.

Loudermilk explained there are a number of noteworthy recent developments in AI that will hopefully be discussed during the hearing. First, the White House Office of Science and Technology Policy (OSTP) recently released principles for how federal agencies can regulate the development of AI in the private sector. He claimed the intent of the principles is to govern AI with the direction on the technical and ethical aspects without stifling innovation. Loudermilk added the principles recommended providing opportunities for public feedback during the rulemaking process considering fairness and nondiscrimination regarding the decisions made by AI applications and basing the regulatory approach on scientific data. He noted that U.S. Chief Technology Officer Michael Kratsios said the principles are designed to ensure public engagement, limit regulatory overreach, and promote trustworthy technology. Loudermilk said some private sector organizations recommend principles for companies using AI, including designating an AI ethics official, ensuring when the customer knows there are interacting with AI, explaining how the AI arrived at its result, and testing AI for bias. He asserted the latter two principles are important for appropriate use of AI by private sector businesses. Loudermilk stated that a basic but central part of explainability is making sure businesses and their regulators are able to know the building blocks of an algorithm when it was being constructed. He added coders should maintain thorough records of what is going into the model when it is being trained ranked by order of importance. Loudermilk said this practice, also known as logging, can isolate sources of bias. Loudermilk stated that a similar concept is present in credit scoring that generates a number that predicts a person's ability to repay a loan. He averred that it is easy to determine why a person's score has gone up or down because the factors that generate a number are transparent.

Loudermilk conceded that recordkeeping is a starting point and not a silver bullet solution to the explainability problem, especially with more complex algorithms. He contended that a key aspect of explainability is defining what fairness is. Loudermilk claimed there needs to be a benchmark to compare algorithm results and evaluate an algorithm's decisions. He said these paper trails can get to the bottom of biases in loan underwiring decisions. Loudermilk stated it is also important to be able to test algorithms to see if there is any bias present, and if there is, a company can take a subset of the data based on sensitive features like gender and race to see if there is disparate impact on a particular group. He stated that aside from testing for bias, testing can also help a company determine if it is arriving at its expected results. Loudermilk stressed it is also important for companies and regulators to verify the input data for accuracy, completeness, and appropriateness. He added that flawed data likely results in flawed algorithm outcomes.

Brookings Institution Fellow Dr. Makada Henry-Nickie stated

> AI-enabled financial technologies are relatively nascent and primarily involve weak or narrow forms of AI. However, financial institutions are increasingly experimenting with advanced deep learning neural networks that are second to none in fitting high volumes of data to extraordinarily accurate predictive functions. Lamentably, deep learning's opaque "Black Box" effect even challenges AI experts when asked two fundamental questions: How? And. Why? These questions are central to human intuition and our cognitive ability to understand and negotiate our environment.
> Beyond philosophical musings, our regulatory system rests firmly on a framework that assesses accountability through a causal lens, to which the answers to the questions of *how* and *why* are crucial for the system to function and effectively serve and protect American consumers. In a causal system, explanations have semantic significance and assist in making connections between reckless judgments or honest mistakes and unfair outcomes. Regulators need to be clear-eyed about an institutional agent's intent to assess the extent of its liability; without clear, rational explanations and clear causal connections between discriminatory outcomes and decision processes, the accountability framework becomes unstable and dysfunctional.

Henry-Nickie stated

> Understandably, AI's black-box effect underpins a growing chorus of calls for intuitive AI explanations between model correlations and biased outcomes. However, explainable AI is not equivalent to the type of transparency we need to redress harms caused by algorithms

> or identify positive lessons to inform the development of equitable algorithms. Achieving an unbiased and impartial algorithm is improbable because machine learning forces the system designer to choose a tolerable balance, based on her preferences or optimization goals.

Henry-Nickie asserted

> A systemic solution that mitigates the harms of biased algorithms continues to escape the legions of AI researchers are aggressively exploring technical solutions to the challenge. Instead, Congress should focus on strengthening, maintaining, and growing the resiliency of the federal consumer oversight framework. Specifically, this task force should take action to strengthen and improve the model governance architecture. Recently, the Government Accountability Office (GAO) concluded that SR 11-7 a mission-critical model risk management framework is subject to review under the CRA. While the effect of GAO's opinion is not immediately apparent, Consumer Financial Protection Bureau's (CFPB) precedent makes it clear that a critical regulatory gap will emerge and potentially weaken regulators' capacity to supervise financial institutions adequately. The task force should encourage CFPB to develop a parallel consumer-focused model governance framework, in light of the proliferation of algorithmic decision-making and marketing tools. Finally, the taskforce should vigilantly monitor the progress of HUD's proposed rule changes to amend the disparate impact standard. The proposed rule introduced five new criteria for establishing disparate impact burdens that, in principle, serve to provide a safe harbor to institutions using algorithms to exploit vulnerable consumers and exacerbate historical disparities.

Attorney and Emerging Tech AI & Privacy Advisor Bärí A. Williams asked "what is AI?" She stated that "[i]t is essentially someone's bias, via datasets, baked into code that can determine the ads one sees, one's credit worthiness, employment prospects, school admissions, housing opportunities, and criminal justice implications (i.e. facial recognition technology, gunshot locaters such as ShotSpotter, predictive policing such as Hunchlab, and predictive sentencing technology)."

Williams stated

> There are five main issues with AI, particularly in financial services: (1) what data sets are being used – who fact checks the fact checkers; (2) what hypotheses are set out to proven using this data – has the narrative that is being written been adequately vetted; (3) how inclusive is the team creating and testing the product – who are you building products with; (4) what conclusions are drawn from the pattern recognition and data that the AI provides – who are you building products for, and who may be harmed or receive benefit, and; (5) how do we ensure bias neutrality, and what is the benefit of neutrality.

Williams asserted

> In our quest to provide greater efficiency and convenience, we have been lax to look at who is left behind and how. If we aren't careful, we will automate greater discrimination into the tools that we use everyday, and further exacerbate the legacy of lack those in marginalized communities. I implore the committee to do a deeper dive into how they can both enforce and enhance the US Equal Credit Opportunity and The Fair Housing Act, in addition to adopting the AI Bill of Rights as attached as Exhibit A.

Carnegie Mellon University Professor Mr. Rayid Ghani stated

> It is critical and urgent for policymakers to act and provide guidelines and/or regulations for both the public and private sector organizations using AI-assisted decision-making processes in order to ensure that these systems are built in a transparent and accountable manner and result in fair and equitable outcomes for society. As initial steps, we recommend:
>
> **1. Expanding the existing regulatory environment to account for AI-assisted decision-making**
>
> The potential risks and benefits of AI to society are as wide and varied as the contexts to which it can be applied. A model or algorithm that yields beneficial and equitable outcomes in one context might yield just the opposite in another. While AI algorithms across different areas have a lot in common, developing a unified regulatory framework for AI that works well across all possible applications is likely to be an unrealistic proposal. Rather, the need for regulatory oversight is inherent in the application of this tool to achieving societal goals across different policy domains.
>
> **Instead of creating a Federal AI regulatory agency across policy areas, we should expand the already existing regulatory frameworks in different policy areas, building on their domain-specific expertise while updating them to account for AI-assisted decision-making.**
>
> The regulatory bodies already exist — including SEC, FINRA, CFPB, FDA, FEC, FTC, and FCC – – and are well-positioned with the responsibility and policy area knowledge for ensuring compliance with existing regulations, but will need to account for new challenges in applying that oversight introduced by the growing application of AI to their domains. These bodies typically regulate the inputs that go into a decision-making process (for example, what attributes cannot be used such as
>
> race or place of residence) and often the processes themselves, but do not always focus on the outcomes produced by these processes. We recommend expanding these regulatory bodies to:
>
> 1. Update the regulations to make them outcome-focused.
> 2. Update the regulations to ensure they apply to AI-assisted decision making.
> 3. Define the set of artifacts an organization (government or industry) should publicly release before deploying (and ideally during the development phases of) an AI system. This includes information on how the system was built, what it was designed to optimize for, what tests were run to check if it did, what types of people is it effective for, who does it fail for, how long was it in trials for, and how did the effectiveness change over time. Ideally this should be put in place for any process involving decision making of any kind, whether human decisions or AI-assisted decisions but becomes critical in cases where the scale of deployed AI systems increases the risk. This set will need to vary based on the impact this system can have on people's lives.
> 4. Define a set of risks that could lead to inequities that need be considered when building an AI system and a mitigation plan for each of these risks.
> 5. Set up an extended data collection process and infrastructure to collect additional data attributes (such as race, gender, or income) that may not already be collected but are necessary to measure equity outcomes (to deal with the "fairness through unawareness" issue described earlier.

6. Set up evaluation standards to compare the performance of these systems to the human decision-making processes currently being used.
7. Define standards around the explainability of the AI systems in order to provide recourse to individuals who may be adversely impacted by the decisions made using the system.

These expanded bodies should be responsible for defining standards as well as for continuous monitoring, audits, and compliance with the standards and regulations.

2. Creating Trainings, Processes, and Tools to Support Regulatory Agencies in their Expanded Roles

As these agencies expand their role, they will need to be supported by increasing their internal capacity to fulfil this role and ensure that regulations are being effectively complied with. We recommend creating trainings, processes, and tools to help them

1. Understand where existing regulations may and may not be well-adapted to applications involving AI-assisted decision-making.
2. Understand and define what equitable outcomes standards to set.
3. Understand how to evaluate whether the requirements created for an AI system were in fact
4. aligned with the identified societal equitable outcomes.
5. Understand how to evaluate whether the AI system did in fact do what it was designed to do.
6. Develop a continuous monitoring and audit process and tools (such as Aequitas19) to support the audit process.
7. Create standards for when a system should "expire" and a corresponding renewal process.

3. Procuring AI systems should include Key Requirements in the Request for Proposals (RFP) Process

Government agencies and corporations putting out RFPs for AI systems that are making critical decisions and affecting people should require proposers/bidders to include:

- An explicit initial project phase to gather requirements for what it would mean to have equitable outcomes and what they should be. This process should include a diverse team and work with stakeholders including: developers who build and deploy AI systems, decision- makers who implement the systems in their workflows, and the community being impacted by these systems.
- A detailed plan and methodology for Steps 1-5 in the previous section of this testimony titled "What does it take to create AI systems that lead to equitable outcomes for society?"
- A continuous improvement plan to ensure that the system continues to not only be evaluated but also improved upon to achieve equitable outcomes.

White House Issues Positioning and Navigation EO

President Donald Trump has issued an executive order (EO), titled "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services," that is designed to drive the development of new and alternative positioning, navigation, and timing (PNT) services (e.g. Global Positioning Systems). If consummated, this initiative could inform federal efforts to drive public sector and private sector of next generation iterations of PNT services for telecommunications, transportation, defense, agriculture, e-commerce, and other areas. Like many of the telecommunications EOs and efforts coming out of the White House, this EO is framed as a critical piece of national security because "the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States." Consequently, the EO links this PNT initiative to the critical infrastructure protection policy framework already in place for policy realms like cybersecurity through reference to Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience.

The EO declares

> It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services. To this end, the Federal Government shall engage the public and private sectors to identify and promote the responsible use of PNT services.

The EO requires a number of federal agencies to take a number of inter-connected actions to drive the development and use of alternative PNT systems as a matter of national security:

- The Department of Commerce "shall develop and make available, to at least the appropriate agencies and private sector users, PNT profiles. The PNT profiles will enable the public and private sectors to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services."
- The Department of Homeland Security "shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services...[and] [t]he results of the tests carried out under that plan shall be used to inform updates to the PNT profiles" developed by the Department of Commerce
- Within 90 days of the PNT profiles being made available, heads of sector-specific agencies and other relevant agencies must "develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services."
- Six months after contractual language is developed, "the Federal Acquisition Regulatory Council, in consultation with the heads of SSAs and the heads of other agencies, as appropriate, shall incorporate [contractual language] into Federal contracts for products, systems, and services that integrate or use PNT services."
- One year after the Department of Commerce makes PNT profiles available, the Department of Homeland Security "shall submit a report to the Assistant to the President for National Security Affairs and the Director of the Office of Science and Technology Policy (OSTP) on the extent to which the PNT profiles have been adopted in their respective agencies' acquisitions and, to the extent possible, the extent to which PNT profiles have been adopted by owners and operators of critical infrastructure."
- Within six months of the EO being issued, "the Secretary of Transportation, Secretary of Energy, and Secretary of Homeland Security shall each develop plans to engage with

critical infrastructure owners or operators to evaluate the responsible use of PNT services...[and] [e]ach pilot program shall be completed within 1 year of developing the plan, and the results shall be used to inform the development of the relevant PNT profile and research and development (R&D) opportunities."

- Within one year of the issuance of this EO, OSTP "shall coordinate the development of a national plan, which shall be informed by existing initiatives, for the R&D and pilot testing of additional, robust, and secure PNT services that are not dependent on global navigation satellite systems (GNSS)...[that] shall also include approaches to integrate and use multiple PNT services to enhance the resilience of critical infrastructure."
- Within six months of issuance of the EO, the Department of Commerce "shall make available a GNSS-independent source of Coordinated Universal Time, to support the needs of critical infrastructure owners and operators, for the public and private sectors to access."

House Homeland Reports Out Legislation To Help State and Local Governments

This week, the House Homeland Security Committee marked up a number of bills, including the "State and Local Cybersecurity Improvement Act" (H.R. 5823), a companion bill to the "State and Local Government Cybersecurity Act of 2019" (S. 1846) that passed the Senate in November 2019. There are significant differences between the bills that would need to be resolved before enactment, and it is possible this happens.

Generally, both bills would create grant programs at the Department of Homeland Security (DHS) to help state and local governments implement better cybersecurity with the impetus being, in part, the rash of ransomware attacks that have recently hit these governments. However, there are substantive differences between the two bills. Notably, the Senate's bill would make entities other than states eligible for financial assistance whereas the House's bill would mainly make states eligible with a means for local governments to apply in case their state does not.

H.R. 5823 would amend the Cybersecurity and Infrastructure Security Agency's (CISA) organic statute by establishing "a program to make grants to States to address cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments." Any state that applies for a grant under this new State and Local Cybersecurity Grant Program must submit a "Cybersecurity Plan" that must include descriptions of how the state will improve the cybersecurity of its information systems, implement a risk-based process to mitigate threats and continuously improve security, drive adoption of best practices and procedures, and pay particular attention to critical infrastructure. These plans would pertain to cybersecurity at the state level and to local, Tribal, and territorial governments within that state. Applying states must also establish cybersecurity planning committees to help draft and implement state Cybersecurity Plans and how to best use any funds in service of these plans.

Before a state can receive a grant, CISA must first approve it. Any state that receives a grant under this program "shall use the grant to implement such State's Cybersecurity Plan, or to assist with activities determined by the Secretary, in consultation with the Director, to be integral to address cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments, as the case may be."

The bill authorizes $400 million per year over five fiscal years for this grant program, but, of course, the Appropriations Committees would need to actually appropriate funds. And, the federal match starts at 90% in the first year and then falls by 10% a year to 50% in the final year for which this program would be authorized.

Within 9 months of enactment, CISA must "develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments that provides recommendations regarding how the Federal Government should support and promote the ability State, local, Tribal, and territorial governments to identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents (as such term is defined in section 2209) and establishes baseline requirements and principles to which Cybersecurity Plans under such section shall be aligned."

As noted, the Senate's companion bill was passed by unanimous consent. The "State and Local Government Cybersecurity Act of 2019," (S. 1846) authorizes DHS "[t]o make grants to and enter into cooperative agreements or contracts with States, local, Tribal, and territorial governments, and other non-Federal…to carry out the responsibilities of the Secretary related to cybersecurity and infrastructure…including grants, cooperative agreements, and contracts that provide assistance and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings." Entities eligible to participate include:

- an association, corporation, whether for-profit or nonprofit, partnership, proprietorship, organization, institution, establishment, or individual, whether domestic or foreign;
- a governmental agency or other governmental entity, whether domestic or foreign, including State, local, Tribal, and territorial government entities; and
- the general public.

CISA's National Cybersecurity and Communications Integration Center (NCCIC) would also be tasked with new, related responsibilities and must "to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center:

- conduct exercises with Federal and non-Federal entities;
- provide operational and technical cybersecurity training related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents to Federal and non-Federal entities to address cybersecurity risks or incidents, with or without reimbursement;
- assist Federal and non-Federal entities, upon request, in sharing cyber threat indicators, defensive measures, cybersecurity risks, and incidents from and to the Federal Government as well as among Federal and non-Federal entities, in order to increase situational awareness and help prevent incidents;
- provide notifications containing specific incident and malware information that may affect them or their customers and residents"

DOJ Claims China Hacked Equifax

The Department of Justice (DOJ) has released a grand jury indictment of four Chinese military hackers for the massive Equifax breach who allegedly "obtain[ed] names, birth dates and social security numbers for nearly half of all American citizens" and Equifax's trade secrets, too. The hackers used a vulnerability in Equifax's Apache Struts Web Framework software and ran thousands of queries to pilfer this information, according to the unsealed grand jury indictment from the U.S. District Court in the Northern District of Georgia in Atlanta. While it is highly unlikely these defendants ever face trial in U.S. court, the announcement will likely create more tension with the

People's Republic of China (PRC) over technology, trade, espionage, and intellectual property issues.

The four defendants were members of the People's Liberation Army's (PLA) 54th Research Institute and "allegedly conspired with each other to hack into Equifax's computer networks, maintain unauthorized access to those computers, and steal sensitive, personally identifiable information of approximately 145 million American victims." Starting in May 2017, the PLA "conspired with each other to hack into the protected computers of Equifax" through a vulnerability in its "online dispute portal that permitted users to research and dispute potential inaccuracies in their Equifax credit reports on servers located in Alpharetta, Georgia." Of course, in March 2017, Apache announced vulnerabilities in its Apache Struts software and released patches. A day after Apache made this announcement, the United States Computer Emergency Readiness Team (US-CERT) released a threat warning notice, advising users to patch the software. However, Equifax did not patch its software, leaving it vulnerable, and the PLA hackers allegedly utilized this failure to patch systems from May-June 2017. Worse still, according to the Federal Trade Commission's July 2019 complaint against Equifax, the company's "security team received the US-CERT alert and, on or about March 9, 2017, disseminated the alert internally by a mass email to more than 400 employees" directing them "to patch the vulnerability within 48 hours, as required by [Equifax's] Patch Management Policy." In late July, according to the FTC Equifax determined there was suspicious traffic on their network, and according to grand jury indictment, the PLA hackers were still exfiltrating information at this point.

Attorney General William Barr made remarks at the press conference to announce the grand jury indictment. He claimed

> This kind of attack on American industry is of a piece with other Chinese illegal acquisitions of sensitive personal data. For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management, the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax. This data has economic value, and these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages.

Barr added that "about 80 percent of our economic espionage prosecutions have implicated the Chinese government, and about 60 percent of all trade secret theft cases in recent years involved some connection to China."

Barr noted that "[w]e do not normally bring criminal charges against the members of another country's military or intelligence services outside the United States...[and] [i]n general, traditional military and intelligence activity is a separate sphere of conduct that ought not be subject to domestic criminal law...[but] [t]here are exceptions to this rule, of course." Barr asserted that "we have charged state-sponsored actors for computer intrusions into the United States for the purpose of intellectual property theft for the use of their private sector, bank robbery, and interfering with our democratic elections...[and] [l]ike those cases, the deliberate, indiscriminate theft of vast amounts of sensitive personal data of civilians, as occurred here, cannot be countenanced."

Moreover, this indictment will undoubtedly be used to lend additional weight to Trump Administration claims that the PRC has been violating the 2015 agreement reached with the Obama

Administration to forgo economic espionage. Of course, the Trump Administration has frequently made the case that the PRC is not living up to the 2015 agreement that it would no longer engage in economic espionage. In May 2018, it made this case extensively in its Section 301 report.

NIST Releases Supply Chain Guidance

The National Institute of Standards and Technology (NIST) has released the Draft National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, for comment. While this document is binding on neither public nor private sector entities, NIST's publications are held in high esteem among stakeholders and are occasionally used by the government as the de facto standard in a field. Moreover, NIST often cross-references guidance documents in a way that amplifies their relevance. For example, as NIST noted in its press release, "[t]he April 2018 update to the NIST Cybersecurity Framework added a new section about supply chain risk management, and the new report cross-references the framework so that organizations can use both sets of NIST guidance together." Comments are due by March 4.

NISTIR 8276 is the latest in a series of Cyber Supply Chain Risk Management (C-SCRM) guidance documents stretching back to the George W. Bush Administration's Comprehensive National Cybersecurity Initiative. NIST explained that "[t]his document provides a set of C-SCRM Key Practices that can be used by any organization...[and] provides guidance as to what these high-level concepts mean, why they are important, and some characteristics and examples of corresponding Key Practices." NIST added that "[t]his document also provides recommendations for how organizations can put the Key Practices into use." NIST added

> In 2018, NIST initiated a set of new, second-generation case studies with the purpose of surveying how the C-SCRM practices evolved and whether new practices emerged. These second-generation case studies were analyzed with the first set of case studies, NIST C-SCRM publications, and numerous industry C-SCRM standards and best practice documents. The results of this analysis revealed that many of the established practices are still relevant, and no practices identified in earlier efforts have been deemed obsolete or retired. This document summarizes the results of this analysis into a set of C-SCRM Key Practices and provides specific recommendations for how to implement them.

In terms of policy background, NIST stated that "[m]any of the recent cyber breaches have been linked to supply chain risks." NIST stated that "[f]or example, a recent high-profile attack that took place in the second half of 2018, Operation ShadowHammer, compromised an update utility used by a global computer manufacturer." NIST asserted that "[t]he compromised software was served to users through the manufacturer's official website and is estimated to have impacted up to a million users before it was discovered." NIST stated that "[t]his is reminiscent of the attack by the Dragonfly group, which started in 2013 and targeted industrial control systems...[and] [t]his group successfully inserted malware into software that was available for download through the manufacturers' websites, which resulted in companies in critical industries such as energy being impacted by this malware." NIST argued that "[t]hese incidents are not just isolated events. Many recent reports suggest these attacks are only increasing in frequency."

NIST contended that "[t]he Key Practices presented in this document can be used to implement a robust C-SCRM function at an organization of any size, scope, and complexity...[and] [t]hese practices combine the information contained in existing C-SCRM government and industry resources with the information gathered during the 2015 and 2019 NIST research initiatives." The Key Practices are:

- Integrate C-SCRM across the organization
- Establish a formal program
- Know and manage your critical suppliers
- Understand your supply chain
- Closely collaborate with your key suppliers
- Include key suppliers in your resilience and improvement activities
- Assess and monitor throughout supplier relationship
- Plan for the full lifecycle

NIST added that "[e]ach key practice includes a number of recommendations, which synthesize how these practices can be implemented from a people, process, and technology perspective...[and] [s]elected key recommendations include:

- Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security (and other relevant) functions.
- Integrate cybersecurity considerations into the system and product lifecycle.
- Determine supplier criticality by using industry standards and best practices.
- Mentor and coach suppliers to improve their cybersecurity practices.
- Include key suppliers in contingency planning, incident response, and disaster recovery planning and testing.
- Use third-party assessments, site visits, and formal certification to assess critical suppliers.

NIST is looking for "feedback on any part of the publication, but there is particular interest in the following:

- The Key Practices and recommendations contained in this publication are intended to be at a level high enough to apply to all types of organizations, regardless of their industry, size, or complexity, yet specific enough to be practical and usable. Are the proposed Key Practices and recommendations at the appropriate level to meet this goal? If not not, how can the document be improved?
- Are there additional Key Practices and recommendations that should be included in this publication and why? Are there Key Practices and recommendations that are currently in the publication that should not be included and why?
- Appendix B includes available government and industry resources that organizations can use to learn more more about C-SCRM. Are there other government or industry resources that should be included and, if so, which ones and why?

House Passes Legislation To Codify Federal Cloud Program

The House passed the “Federal Risk and Authorization Management Program Authorization Act of 2019” (H.R. 3941) that would codify the Federal Risk and Authorization Management Program at the General Services Administration (GSA) and “authorize GSA to establish a governmentwide program to provide a standardized approach to security assessment and authorization for cloud computing products and services” according to the Committee Report. At present, there is no companion bill in the Senate. House Oversight and Reform Committee’s Government Operations Chair Gerry Connolly (D-VA) and Ranking Member Mark Meadows (R-NC) cosponsored the bill.

According to the Committee Report, H.R. 3941 would

- direct the Administrator of GSA to establish a governmentwide program to provide the authoritative standardized approach to security assessment and authorization of cloud computing products and services that process unclassified information used by agencies.
- assign roles and responsibilities in providing guidance and administering the program to GSA, the FedRAMP Program Management Office (PMO), the Joint Authorization Board (JAB), independent assessment organizations, and the Office of Management and Budget (OMB).
- require an annual report to Congress on the efficiency and effectiveness of the FedRAMP PMO and agencies in supporting the effectiveness and security of authorizations to operate for cloud computing products and services and other information such as the number of authorized cloud computing services in use at each agency.
- authorize to be appropriated $20 million for the FedRAMP program.
- establish a Federal Secure Cloud Advisory Committee to ensure effective and ongoing coordination of agency adoption, use, authorization, monitoring, acquisition, and security of cloud computing products and services to enable agency mission and administrative priorities.

NIST Details Zero Trust Concept

The National Institute of Standards and Technology (NIST) has released for comment Draft (2nd) NIST Special Publication (SP) 800-207, Zero Trust Architecture, and wants interested parties to respond by email (zerotrust-arch@nist.gov) by March 13, 2020, ideally using the provided comment template. NIST explained that this draft SP "discusses the core logical components that make up a zero trust architecture (ZTA) network strategy…[and] builds upon the first draft with a new section on zero trust approaches as well as updates to material based on public comments." NIST stated that "[t]his is the product of a collaboration between multiple federal agencies and is overseen by the Federal CIO Council." When finalized, this SP would not supersede any of the binding requirements imposed on federal agencies or contractors as detailed in Office of Management and Budget (OMB) memoranda and FIPS publications. However, NIST is seeking to drive the debate and develop government policy on better securing the systems, information, and data used by or behalf of federal agencies.

NIST explained that "[z]ero trust refers to an evolving set of network security paradigms that narrows defenses from wide network perimeters to individual resources…[and] [i]ts focus on protecting resources rather than network segments is a response to enterprise trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary." NIST said "[a]n operative definition of zero trust and zero trust architecture is as follows:

> Zero trust (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

NIST stated that "[t]his publication discusses ZTA, its logical components, possible deployment scenarios, and threats...[and] also presents a general road map for organizations wishing to migrate to a zero trust design approach to network infrastructure and discusses relevant federal policies that may impact or influence a zero trust architecture strategy." NIST claimed that "ZT is not a single-network architecture but a set of guiding principles in network infrastructure and system design and operation that can be used to improve the security posture of any classification or sensitivity level."

NIST remarked that "[a] typical enterprise's infrastructure has grown increasingly complex...[and] [a] single enterprise may operate several internal networks, remote offices with their own local infrastructure, remote and/or mobile individuals, and cloud services." NIST stated that "[t]his complexity has outstripped traditional methods of perimeter-based network security as there is no single, easily identified perimeter for the enterprise...[and] [p]erimeter-based network security has also been shown to be insufficient since once attackers breach the perimeter, further lateral movement is unhindered." NIST said that "[t]his complex enterprise has led to the development of a new model for cybersecurity principles and network security known as "zero trust" (ZT)." NIST said that "[a] ZT approach is primarily focused on data protection but can be expanded to include all enterprise assets, such as devices, infrastructure, and users." NIST said that "[z]ero trust security models assume that an attacker is present on the network and that an enterprise-owned network infrastructure is no different—or no more trustworthy—than any nonenterprise-owned network." NIST stated that "[i]n this new paradigm, an enterprise must continually analyze and evaluate the risks to its internal assets and business functions and then enact protections to mitigate these risks. In zero trust, these protections usually involve minimizing access to resources (such as data and compute resources and applications) to only those users and assets identified as needing access as well as continually authenticating and authorizing the identity and security posture of each access request."

NIST stated that "[f]ederal agencies have been urged to move to security based on zero trust principles for more than a decade, building capabilities and policies such as the Federal Information Security Modernization Act (FISMA) followed by the Risk Management Framework (RMF); Federal Identity, Credential, and Access Management (FICAM); Trusted Internet Connections (TIC); and Continuous Diagnostics and Mitigation (CDM) programs." NIST stated that "[a]ll of these programs aim to restrict data and resource access to authorized parties." NIST stated that "[w]hen these programs were started, they were limited by the technical capabilities of information systems...[and] [a]s technology matures, it is becoming possible to continually analyze and evaluate access requests in a dynamic and granular fashion to a "need to access" basis to mitigate data exposure due to compromised accounts, attackers monitoring a network, and other threats."

Administration's Data Strategy Action Plan

The Trump Administration has released its 2020 Action Plan for implementation of its Federal Data Strategy. A draft Action Plan was released for comment in June 2019. The Administration claimed the 2020 Action Plan "establishes a solid foundation that will support implementation of the strategy over the next decade...[and] identifies initial actions for agencies that are essential for establishing processes, building capacity, and aligning existing efforts to better leverage data as a strategic asset." The use of federal data holds a key place in the President's Management Agenda (PMA) and, according to the Administration, will be a key driver in transforming how the federal government operates, particularly in relation to technology. The 2020 Action Plan lays out the steps agencies will be expected to take to realize the Administration's 10-year Federal Data Strategy.

As always, results will be informed by follow through and prioritization by the Office of Management and Budget (OMB) and buy-in from agency leadership.

Notably, the Administration tied the 2020 Action Plan to a number of other ongoing initiatives that rely heavily on data. The Administration said the plan "incorporates requirements of the Foundations for Evidence-Based Policymaking Act of 2018, the Geospatial Data Act of 2018, and Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence." The Administration also explained that "[b]ecause the governing laws vary in scope and applicability, the actions described in this policy document below, differentiate between actions that are mandatory and those that are strongly encouraged."

The substance of the 2020 Action Plan is divided into three sections: Agency Actions, Community of Practice Actions, and Shared Solution Actions. The Administration explained the three categories this way:

- 6 Agency Actions are executed by each agency and are designed to advance each agency's ability to fully leverage its data as a strategic asset. Agency Actions set expectations for progress and success in implementing the strategy by building a foundation for the management of data throughout the lifecycle within agencies Implementation guidance will be routinely updated on strategydata.gov, and resources to support implementation will be regularly posted to the repository at resourcesdata.gov
- 4 Community of Practice Actions are taken by a specific group of agencies around a common topic, usually through an established interagency council or other existing coordinating mechanism Community of Practice Actions seek to integrate and coordinate ongoing efforts related to existing laws, regulations, and executive orders that are particularly relevant to the strategy
- 10 Shared Solution Actions are distinct projects or efforts that are led by a single agency or existing interagency council for the benefit of all agencies. Shared Solution Actions provide government-wide thought leadership, direction, tools, governance, and services for implementing the strategy that can be leveraged by all agencies Many of the Shared Solution Actions have received financial resources as part of the CAP Goal: Leveraging Data as a Strategic Asset and are already underway.

And, the Administration detailed the specific actions within the three sections agencies will either be required or encouraged to take:

- Agency Actions
    - Action 1: Identify Data Needs to Answer Priority Agency Questions
    - Action 2: Constitute a Diverse Data Governance Body
    - Action 3: Assess Data and Related Infrastructure Maturity
    - Action 4: Identify Opportunities to Increase Staff Data Skills
    - Action 5: Identify Priority Data Assets for Agency Open Data Plans
    - Action 6: Publish and Update Data Inventories
- Community of Practice Actions
    - Action 7: Launch a Federal Chief Data Officer Council
    - Action 8: Improve Data and Model Resources for AI Research and Development
    - Action 9: Improve Financial Management Data Standards
    - Action 10: Integrate Geospatial Data Practices into the Federal Data Enterprise
- Shared Solution Actions
    - Action 11: Develop a Repository of Federal Enterprise Data Resources

- Action 12: Create OMB Federal Data Policy Committee
- Action 13: Develop a Curated Data Skills Catalog
- Action 14: Develop a Data Ethics Framework
- Action 15: Develop a Data Protection Toolkit
- Action 16: Pilot a One-stop Standard Research Application
- Action 17: Pilot an Automated Tool for Information Collection Reviews that Supports Data Inventory Creation and Updates
- Action 18: Pilot Enhanced Data Management Tool for Federal Agencies
- Action 19: Develop Data Quality Measuring and Reporting Guidance
- Action 20: Develop a Data Standards Repository

In June 2019, the OMB released the Federal Data Strategy and the Administration released a draft Action Plan. OMB explained that "[t]he Strategy complements statutory requirements (such as the E-Government Act of 2002, the Privacy Act of 1974, and the Federal Information Security Modernization Act of 2014) and OMB information policy and guidance (such as OMB Circular A-130 Managing Information as a Strategic Resource.) In fall 2018, the Department of Commerce released a request for comments on the practices of a new Federal Data Strategy as part of the Trump Administration's Cross-Agency Priority (CAP) goal of "Leveraging Data as a Strategic Asset." This CAP goal is one of the pillars of the White House's PMA that "lays out a long-term vision for modernizing the Federal Government in key areas that will improve the ability of agencies to deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars on behalf of the American people." This CAP goal seeking to change how data is used also entails, in significant part, addressing how the federal government manages and handles data. Moreover, any CAP goal may drive agency policy changes to align their data procedures and processes with the Administration's priorities.

OMB explained that Federal Data Strategy is "a framework of operational principles and best practices that help agencies deliver on the promise of data in the 21st century." OMB explained that "[t]hrough consistent data infrastructure and practices, the Strategy will enable Government to fully leverage data as a strategic asset by supporting strong data governance and providing the protection and security that the American people, businesses, and partners deserve." OMB stated that "[t]he Strategy is comprised of three components to guide Federal data management and use:

- Mission Statement: The mission statement articulates the intent and core purpose of the Strategy.
- Principles: The principles serve as motivational guidelines in the areas of Ethical Governance, Conscious Design, and Learning Culture. They include concepts from existing frameworks, such as protecting personally identifiable information, managing information as an asset, carrying out fundamental responsibilities of a Federal statistical agency, and building Federal evidence.
- Practices: The practices guide agencies in leveraging the value of data by Building a Culture that Values Data and Promotes Public Use; Governing, Managing, and Protecting Data; and Promoting Efficient and Appropriate Data Use.

Many stakeholders have long called for the federal government to better make available its data sets for a range of reasons, including providing the data necessary to bring about further and greater use of artificial intelligence and machine-learning, to name just two applications in need of more data. It remains unclear the extent to which this program will be implemented and how much data will be utilized by the public and private sectors.

NDAA-Required Indo-Pacific Study Released

The Center for a New American Security (CNAS) has released a study required by the FY 2019 National Defense Authorization Act (NDAA) (P.L. 115-232) on how the geopolitical conditions in the Indo-Pacific region affect implementation of the National Defense Strategy released in 2018. Not surprisingly, almost the entire report focuses on China, and a good portion of it highlights a range of technology-related issues, including supply chain, 5G, rare earth minerals, Chinese tech companies, technology transfers, and others. CNAS offered a range of policy recommendations to the DOD and other agencies in particular and the Trump Administration in general, but, of course, it remains to be seen which may be adopted and implemented, if any. Nonetheless, these recommendations may form the basis for further language in an NDAA regarding China, so it does bear scrutiny on that basis alone.

The Department of Defense (DOD) was required to contract with an independent think tank and chose CNAS to perform the work. Specifically, Section 1254 of the FY 2019 NDAA required the DOD to retain "an entity independent of the Department of Defense to conduct an assessment of the geopolitical conditions in the Indo-Pacific region that are necessary for the successful implementation of the National Defense Strategy." In particular, this assessment should include such "a determination of the geopolitical conditions in the Indo-Pacific region, including any change in economic and political relations, that are necessary to support United States military requirements for forward defense, assured access, extensive forward basing, and alliance and partnership formation and strengthening in such region." In its preface, CNAS made the claim that "is intended to help close the considerable gap between the current administration’s stated aspirations for a free and open Indo-Pacific and the actual implementation of policies to advance that vision."

As noted, CNAS made a range of recommendations, some of which are military, diplomatic, trade, or economic; however, there are a number of technology-related recommendations that, if implemented by the Trump Administration, would bear directly or indirectly on technology companies. In Chapter II ("Securing Vital U.S. Technological Advantages,") CNAS made the following overall observations:

- Advanced technology translates directly into military and economic power, and further provides leading nations with the ability to shape international norms and domestic governance practices. Sustaining America’s technological edge will therefore be vital to realizing a free and open Indo-Pacific. Fortunately, the United States retains a number of advantages in the technological competition with China: world-class universities and research institutes, leading technology companies, a vibrant venture capital and start-up ecosystem, and a long history of rewarding innovation. America has also benefited profoundly from being a place where people from around the world want to work and live.
- Yet, largely due to choices in Washington and Beijing, America’s position as the global technology leader is under threat. U.S. expenditures on research and development have stagnated for decades as a share of gross domestic product (GDP). In the meantime, China has quadrupled its spending and is on the brink of surpassing the United States in total investments in this area. Already, the results are showing: China is now a global powerhouse in a number of strategic technologies, equal to or ahead of the United States in critical areas such as quantum computing, artificial intelligence, and genomics. If current trends continue, the downstream military, economic, and political consequences could tip the scales toward China’s vision of regional order in the Indo-Pacific.

In order to remedy this state of affairs, CNAS claimed:

- To keep apace, Washington will have to do more to reinvigorate American technological leadership. The U.S. government should set ambitious national goals for public and private spending on research and development, while bolstering human capital and high-skilled immigration. Relying on competitive, market-oriented principles—and avoiding a heavy-handed industrial policy in which the government picks winners and losers—Washington should provide resources and data to defend and advance key areas of U.S. competitive advantage, including artificial intelligence and semiconductors. As it reinvigorates its innovation base at home, the United States will have to be more vigilant in protecting key U.S. technologies. Recent legislative efforts to enhance U.S. investment screening and export controls are a good start and must be followed through. But more comprehensive efforts are still needed to address China's harmful and illicit practices of forced technology transfer, academic and commercial espionage, and intellectual property theft. Washington will have to establish a more productive and collaborative relationship with U.S. businesses and universities. It will also be necessary to augment resources for counterespionage investigations and visa screening, as well as a demonstrated willingness and ability to retaliate against Chinese firms and individuals that benefit from technology theft.
- Critically, going it alone will be insufficient for the United States, both because of China's economies of scale and because unilateral defensive measures will be ineffective if Beijing can easily exploit other advanced economies. Washington should lead on establishing a new international body of democratic powers to coordinate on technology policy and develop cooperative solutions to combating China's anti-competitive practices. Sustaining U.S. technological advantages will also require the United States to be more proactive internationally in setting new rules around emerging technologies. Active U.S. participation in international standards-setting bodies will be essential. Meanwhile, the United States can lead efforts in the Indo-Pacific and globally to codify norms for the use of emerging technologies. This should include detailed discussions with Beijing over the future of artificial intelligence.

In terms of specific recommendations for Chapter II (Securing Vital U.S. Technological Advantages), CNAS offered the following:

- **Bolster America's innovation engine (p. 21)**
  - Increase research and development investments in the United States.
  - Accelerate U.S. innovation in artificial intelligence through standards-setting, metrics, and horizon-scanning.
  - Support U.S. innovation in artificial intelligence and machine learning by increasing the availability of government data and computing resources.
  - Forge an alliance innovation base.
- **Protect critical U.S. technological advantages (p. 22)**
  - Secure semiconductor supply chains.
  - Establish multilateral export controls on semiconductor manufacturing equipment and increase federal funding for next-generation hardware.
  - Diversify sources of rare earth minerals.
  - Expand export controls based on end use for certain products sold to China.
- **Counter illicit technology transfer (p. 24)**
  - Ensure sufficient resources for counterespionage investigations.
  - Develop better collaboration between U.S. law enforcement and universities.

- Improve visa screening for espionage risks.
    - Expand sanctions authorities to cut o from the U.S. market and financial system Chinese firms that steal U.S. technology.
    - Include more People's Liberation Army-linked companies on the export regime Entity List.
- **Lead on developing new international rules, norms, and standards for emerging technologies (p. 25)**
    - Create a new grouping of advanced democracies to coordinate on technology policy.
    - Engage more proactively in multilateral bodies that set technology standards.
    - Lead internationally and engage with China on developing norms and principles for the use of emerging technologies.

In Chapter VI (Promoting Digital Freedom and Countering High-Tech Illiberalism), CNAS turns to other technology-based issues and made these recommendations:

- **Bolster America's digital engagement in the Indo-Pacific (p. 44)**
    - Establish a new U.S. Digital Development Fund that would, in coordination with allies, support information connectivity projects in the Indo-Pacific and beyond.
    - Direct the new U.S. International Development Finance Corporation to support projects in the Indo-Pacific that provide alternatives to China's digital infrastructure.
    - Augment U.S. digital diplomacy in the Indo-Pacific with additional digital attachés and high-level "digital delegations."
- **Prevent China's dominance of digital infrastructure in the Indo-Pacific (p. 45)**
    - Revitalize global competition in 5G wireless technology.
    - Increase pressure on Huawei's 5G ambitions while honing the current U.S. approach to the company.
    - Actively reject the notion of "internet sovereignty" and advance access to fact-based information as a universal human right.
- **Challenge China's surveillance state domestically and overseas (p. 46)**
    - Leverage America's economic toolkit to target actors facilitating the spread of China's high-tech illiberalism.
    - Design new means to circumvent China's "Great Firewall."
    - Promote independent media, civil society, and government accountability throughout the Indo-Pacific

As mentioned, which, if any, of these recommendations are implemented by the Trump or folded into the FY 2021 NDAA in one form or another.

Further Reading

- "'The intelligence coup of the century'" – *The Washington Post*. A fascinating read of how the Central Intelligence Agency and National Security Agency and West Germany's intelligence agency used a Swiss company, Crypto AG, to sell encryption machines to the governments of many countries that enabled the agencies to spy on their communications. This operation ran from the mid-1950's through the last decade when end-to-end encryption in apps and devices rendered such machines superfluous. According to the source documents and sources, the Germans were appalled by the Americans insistence that even allies be spied upon. The revelations in this article may not help the Trump Administration make the case that Huawei and other Chinese companies are security risks.

- "Ransomware Attacks Grow, Crippling Cities and Businesses" – *The New York Times*. Experts continue to insist the actual number of ransomware attacks are underreported for a variety of reasons, including the fact many victims pay the ransom. However, the reported number of attacks and the average amount of demanded ransom continues to grow. Hackers are growing more creative in who they target and how they try to get payment. Worse still, these attacks are driving a number of smaller and mid-sized businesses to close down when they either choose not to pay the ransom or do not get their data unlocked, a common occurrence.
- "Explained: Why The Feds Are Raiding Tech Companies For Medical Records" – *Forbes*. Law enforcement agencies are making requests of and receiving access from companies that hold vast amounts of medical records. This seems to be an area of data privacy that has not received much attention.
- "U.S. Officials Say Huawei Can Covertly Access Telecom Networks" – *Wall Street Journal*. According to British, German and U.S. officials, the Trump Administration has been providing evidence that Huawei maintains access through its hardware to telecommunications systems. However, Administration officials would not say whether Huawei or Chinese intelligence has used this access. Huawei denied ever having spied and asserted it would not heed Chinese intelligence if directed to do so. The company did not say whether it has or would allow Chinese intelligence operatives to access these alleged backdoors. Nonetheless, even with this purported evidence, both the U.K. and Germany appear to be willing to use Huawei equipment with certain security mitigation.
- "California's new privacy law is off to a rocky start" – *TechCrunch*. There continues to be a wide range of compliance with the "California Consumer Privacy Act" (AB 375) and a nascent subindustry of tech companies to help California residents utilize their rights under the new privacy statute.
- "Judge orders Pentagon to stop work on JEDI cloud contract" – *Politico*. A federal court granted Amazon's request to enjoin the Department of Defense's $10 billion Joint Enterprise Defense Infrastructure cloud contract that was awarded to Microsoft. Amazon has argued that President Donald Trump's tweets and other actions prejudiced the company during the procurement. It remains to be seen whether Amazon will prevail.
- "How Big Companies Spy on Your Emails" – *Vice's Motherboard*. Turns out your email may be the subject of data mining and subsequent sharing of information gleaned from inboxes. The companies identified in the article claim they only utilized anonymized or pseudonymized data.
- "Personal Data of All 6.5 Million Israeli Voters Is Exposed" – *The new York Times*. An app used by Prime Minister Benjamin Netanyahu's Likud Party made available the personal information of every voter in Israel through apparently shoddy data security or a mistake. White hat hackers flagged the problem, but it is not clear who, if anyone, may have accessed the information.