Michael Kans' Technology Policy Update
12 June 2019
By Michael Kans, Esq.

House Oversight Hearing on Facial Recognition

Last week, the House Oversight and Reform Committee held its second hearing in a series on facial recognition technology, which a bipartisan consensus on the committee agree present Constitutional issues as currently deployed. In the previous hearing, Members decried the lack of federal oversight of federal, state, and local law enforcement agencies' use of the technology to identify, track, trace, and locate Americans and others given the widely documented problems with respect to correctly identifying women and minorities. The chair has articulated his plan that the subcommittees will divvy up the policy area, hold hearings, and then generate policies to address the problems and concerns turned up during the hearing. However, even should the committee and then the House produce legislation, like most bills passed by the House, the Senate may not take up such legislation.

The witnesses that testified before the committee were:

- Federal Bureau of Investigation Deputy Assistant Director Kimberly J. Del Greco
- Director, Government Accountability Office Homeland Security and Justice Director Dr. Gretta Goodwin
- Transportation Security Administration Assistant Administrator Austin Gould
- National Institute of Standards and Technology Information Technology Laboratory Director Dr. Charles Romine

Chair Elijah Cummings (D-MD) stated the committee is holding its second hearing on the sue of facial recognition technology that would focus on the use of this technology by law enforcement agencies across the federal government. He noted the committee has heard from experts on the benefits and dangers of this technology across the government and private sector. Cummings said the committee concluded after this first hearing that facial recognition technology is rapidly developing without any real safeguards. He asserted that use of the technology by government and commercial entities poses risks to civil rights and liberties and Americans' right to privacy. He noted both Republicans and Democrats are concerned about facial recognition technology and there is wide-ranging agreement that the committee should be conducting oversight to develop common sense proposals. Cummings said the committee is uniquely situated to take a government-wide view on facial recognition technology. He noted an April letter sent by the Government Accountability Office (GAO) to the Department of Justice with open recommendations on the Federal Bureau of Investigation's (FBI) use of facial recognition technology that were made three years ago. Cummings remarked the committee would also hear from the Transportation Security Administration (TSA) about its pilot program that subjects Americans to facial recognition technology in some airports. He said each subcommittee has been tasked with a discrete policy area to investigate such as civil rights and civil liberties or safeguarding consumers.

Ranking Member Jim Jordan (R-OH) said two weeks ago the committee learned that facial recognition technology disproportionately affects African Americans, raises First and Fourth Amendment concerns when used by the FBI and federal government, and impinges Due Process rights when used by the FBI and federal government. He added that over 20 states have given the FBI access to their department of motor vehicles' data base, and in many cases, no one signed off

on this decision. Jordan said no Americans agreed to this decision and no elected officials voted to allow this to happen. He contended that the FBI has neglected to implement the GAO's recommendations over the last three years. Jordan the expansion of the use of facial recognition technology is happening in a nation with 50 million surveillance cameras.

Del Greco claimed that "[f]acial recognition is a tool that, if used properly, can greatly enhance law enforcement capabilities and protect public safety, but if used carelessly and improperly, may negatively impact privacy and civil liberties. She stated that "[t]his is why when the FBI developed the use of facial recognition technologies, it also pioneered a set of best practices, so that effective deployment of these technologies to promote public safety can take place without interfering with our fundamental values." Del Greco said that "[k]ey points of the FBI's use of facial recognition include the following:

- FBI policy strictly governs the circumstances in which facial recognition tools may be utilized, including what probe images may be used.
- FBI uses facial recognition technology for law enforcement purposes with human review and additional investigation. The FBI's use of facial recognition produces a potential investigative lead and requires investigative follow-up to corroborate the lead before any action is taken.
- Every face query--including results received from our partners--is reviewed and evaluated by trained examiners at the FBI to ensure the results are consistent with FBI standards.
- The FBI is committed to ensuring that FBI facial recognition capabilities are regularly tested, evaluated, and improved. In addition to system testing, the FBI has partnered with NIST to ensure algorithm performance is evaluated.

Goodwin stated that "[i]n May 2016, GAO found that the DOJ and the FBI could improve transparency and oversight to better safeguard privacy and had limited information on accuracy of its face recognition technology…[and] GAO made six recommendations to address these issues." She claimed that "[a]s of May 2019, DOJ and the FBI had taken some actions to address three recommendations—one of which the FBI has fully implemented—but has not taken any actions on the other three." Goodwin stated that "[i]n its May 2016 report, GAO found that DOJ did not complete or publish key privacy documents for FBI's face recognition systems in a timely manner and made two recommendations to DOJ regarding its processes for developing these documents:"

- These included privacy impact assessments (PIA), which analyze how personal information is collected, stored, shared, and managed in federal systems, and system of records notices, which inform the public about, among other things, the existence of the systems and the types of data collected. DOJ has taken actions to expedite the development process of the PIA. However, DOJ has yet to take action with respect to the development process for SORNs. GAO continues to believe both recommendations are valid and, if implemented, would help keep the public informed about how personal information is being collected, used and protected by DOJ components.
- GAO also recommended the FBI conduct audits to determine if users of FBI's face recognition systems are conducting face image searches in accordance with DOJ policy requirements, which the FBI has done.

Goodwin added that "GAO also made three recommendations to help the FBI better ensure the accuracy of its face recognition capabilities:

- First, GAO found that the FBI conducted limited assessments of the accuracy of face recognition searches prior to accepting and deploying its face recognition system. The face recognition system automatically generates a list of photos containing the requested number

of best matched photos. The FBI assessed accuracy when users requested a list of 50 possible matches, but did not test other list sizes. GAO recommended accuracy testing on different list sizes.

- Second, GAO found that FBI had not assessed the accuracy of face recognition systems operated by external partners, such as state or federal agencies, and recommended it take steps to determine whether external partner systems are sufficiently accurate for FBI's use. The FBI has not taken action to address these recommendations. GAO continues to believe that by verifying the accuracy of both systems—its system, and the systems of external partners—the FBI could help ensure that the systems provide leads that enhance criminal investigations.
- Third, GAO found that the FBI did not conduct an annual review to determine if the accuracy of face recognition searches was meeting user needs, and recommended it do so. In 2016 and 2017 the FBI submitted a paper to solicit feedback from system users. However, this did not result in formal responses from users and did not constitute a review of the system. GAO continues to believe that conducting such a review would help provide important information about potential factors affecting accuracy of the system.

Senate Banking Looks At China's Technology Practices and Opioid Production

On June 4, the Senate Banking, Housing, and Urban Affairs Committee held a hearing titled "Confronting Threats From China: Assessing Controls on Technology and Investment, and Measures to Combat Opioid Trafficking." In holding this hearing, the committee united two discrete policy areas not typically considered together: China's practices visa vis western technology firms and production of opioids in China that are subsequently exported to the U.S. The combination of this issues probably says more about the composition of the committee than it does about the similarity of the policy challenges produced by these two practices.

The committee heard from the following witnesses:

- Former Assistant Secretary of Commerce for Export Administration in the Bureau of Industry and Security (BIS) Kevin Wolf
- Center for Strategic & International Studies Senior Adviser Scott Kennedy
- Former Principal Deputy Coordinator for Sanctions Policy at the Department of State Richard Nephew

Chair Mike Crapo (R-ID) stated that "[i]n a very short span, Beijing has managed to transform itself from the perennial hope of being a cooperative trade partner to an all-out strategic competitor, in part, to confront China's industrial policy program, which, among other things, includes subsidies for its domestic companies developing advanced semiconductors, the bedrock of all things, today." He said that "[w]orse still, China is one of the United States' largest trading partners and it is in part pursuing that policy through a concept known as 'civil-military fusion,' which is intended to provide the missing link between China's technological and military rise." Crapo stated that "[m]ore and more, U.S. national security grounds are called upon to confront threats to America's dominance in high technology manufacturing and other threats from China." He explained that "the Committee will focus on three threats from China:

- The first two threats arise from emerging national security issues associated with foreign investment in the United States and the export of critical technologies, particularly in the semiconductor industry, which is a primary target for illicit acquisition. Last year, the Committee successfully negotiated and the President signed into law The Foreign Investment Risk Review Modernization Act (FIRRMA) and the Export Control Reform Act (ECRA).

Together, this bipartisan, bicameral legislation works to enhance the federal government's authorities to protect America against illicit foreign investments in, acquisitions of, and transfers of America's most sensitive technologies. Today, the committee will hear from a variety of perspectives on whether these new laws are sufficient to counter China's threats, or if other measures must be considered. Of particular interest is the question of how we separate and protect U.S cutting edge technology from the non-national security related trade that finances America's greatest innovative achievements.

- The third threat we will focus on involves the supply of fentanyl to the United States, which is causing close to 38,000 American deaths a year, now.

Ranking Member Sherrod Brown (D-OH) stated that "[t]oday we will focus on whether to provide the administration with new sanctions tools to complement existing Foreign Narcotics Kingpin sanctions, targeting traffickers in China, Mexico, and elsewhere who are contributing to the rising tide of illicit opioids coming into the US, including powerful new forms of fentanyl." He added that "[w]e will also address today the range of challenges posed by China in export control, intellectual property theft, technology transfer, and certain foreign investments–including through China's massive Belt and Road Initiative, its Made in China 2025 initiative, and targeted collaborative investments in U.S. firms with critical technologies that China seeks to acquire." Brown claimed that "[w]e must respond forcefully when China's ambitious and sometimes illegal acquisition strategies are deployed against U.S. firms, raising critical national security or economic security questions here at home." He contended that "[t]his is what we did last year when we passed the Foreign Investment Risk Review Modernization Act—updating and expanding both the Committee on Foreign Investment in the United States, and export control laws…[and] [a]lmost a year after enactment of these reforms, we'll hear testimony that some foreign investors continue trying to capture the intellectual property of leading edge U.S. technology companies for their home country's military uses, or worse, to disrupt U.S. supply chains."

Wolf said that "[t]he United States has always pursued two complementary objectives – protecting our national security and promoting U.S. technology leadership. " He stated that "[w]hile they both make us stronger, they have very different tools and purposes…[and] [w]e have spent 50 years building a global trading system with clear rules and tools for remedying unfair trade practices. Export controls are not one of them." Wolf stated that "[i]f we use export control-related national security justifications for purely trade policy purposes, we will undermine the system we have built and even further encourage the Chinese government to do so even more." He explained that "[e]xport controls should be used to their fullest possible extent, however, when a specific national security or foreign policy issue pertains to the export, reexport, or transfer of commodities, technologies, software, or services to destinations, end users, or end uses." Wolf asserted that "[i]f the issue pertains to an activity, an investment, or a concern separate from such events or concerns, then one must look to other areas of law, such as sanctions, trade remedies, foreign direct investment controls, intellectual property theft remedies, or counter-espionage laws." He stated that "[i]n addition, a trade agreement among Pacific allies surrounding China could be a useful tool in motivating, through collective multilateral action, changes in unfair Chinese trade activities – while, at the same time, benefiting U.S. industry's access to such markets and projecting American labor and environmental protection values." He said that "[r]eturning to the title of the hearing – assessing controls on investments and technology relevant to threats involving China – the key to doing so properly is more funding for more people in BIS and the other export control agencies to regularly and aggressively conduct and implement such assessments." Wolf stated that "[i]n light of broad grants of authority in ECRA and FIRRMA, I do not yet believe more law is needed to do so." Wolf stated that "[t]he issues and technologies involving China are more complex than ever and the need

for multilateral cooperation, which is time intensive, continues to remain extremely important to the controls' effectiveness…[and] I believe that each agency is understaffed when compared to its mission." Wolf stated that "[a]mong other things, this leads to increased burdens and delays for industry, reduced time needed for internal training, insufficient time to study all the issues; and the inability to keep the regulations current…[and] [f]ailure to keep the regulations current to novel threats does not advance our national security interests and harms our economic security."

Kennedy contended that "one of the largest lessons I take from my years of working on China and US-China relations is our need to adopt a posture of principled pragmatism: we need to be guided by our values, but we also need to be smart in how we pursue them." He asserted that "[a] clear purpose needs to be married to well-reasoned and effective policy…[and] [o]ur purpose should be to encourage and press for humane governance in China domestically and its responsible behavior internationally." Kennedy stated that "[p]ursuing these goals requires a combination of engagement with China, deterrence and opposition to some of its policies and actions, and collaboration with friends and allies in the Asia-Pacific and beyond." He claimed that "[b]ut most importantly, success requires making America the best it can be…[and] [o]ur direct effect on China will always be limited." Kennedy said that "[w]e have a much greater ability to make our own economic, social and political systems stronger, serve as a model for others, and have them recognize how their national interests are best served by having a good relationship with the United States."

Kennedy said that "[i]n a narrow sense, current American policy appears to overestimate China's high-tech prowess, but it probably makes sense to err on the side of caution and prepare for a China that once again defies expectations to overcome many of the challenges described above." He said that "[t]hat said, the Trump Administration's approach to responding to China's high-tech challenge is overly focused on a single approach: pressure…[and] [t]his stance is understandable given China's highly aggressive approach that threatens the health of individual companies as well as entire industry supply chains and business models." Kennedy stated that "[u]nder Xi Jinping China has made some modest adjustments to market access in some industries, for example, gradually reducing joint-venture requirements for automobiles and liberalizing access to its financial markets, but the overall trajectory is one of greater control and discrimination against foreign industry."

House FY 2020 Homeland Security Bill Starts To Move

Last week, the House Appropriations Committee began to move its FY 2020 Homeland Security appropriations package, one of the last bills to be considered by the committee during this cycle. The committee opted to reject the Administration's proposed funding cut for the agency inside the Department of Homeland Security (DHS) that assists the cybersecurity of much of the federal civilian government and serves as the federal government's information sharing hub. The Cybersecurity and Infrastructure Security Agency (CISA) would receive $2.016 billion for FY 2020, a boost of $334 million above its FY 2019 funding level and $408 million above the Administration's budget request. However, the final funding measure that appropriates money for DHS will likely be among the final decisions made in the FY 2020 appropriations cycle as the White House continues to use funds appropriated for other purposes for construction of a border wall and have requested funds for the next fiscal year to do the same. House Democrats have rejected both, and their package does not provide funding for a border wall, setting up another clash with President Donald Trump.

The subcommittee with jurisdiction over a number of agencies and programs also marked up the FY 2020 Financial Services and General Government appropriations act, sending it to the full committee.

In a summary, the subcommittee explained the bills highlight's, including

- **Election Assistance Commission (EAC) –** The bill provides $600 million for **Election Security Grants** to augment state efforts to improve the security and integrity of elections for Federal office. In addition, $16.2 million is included for EAC operating expenses, an increase of $7 million above the 2019 enacted level and $4.2 million above the President's budget request.
- **Federal Trade Commission (FTC)** – The bill includes $349.7 million for the FTC, which is $40 million above the 2019 enacted level, to bolster antitrust and consumer protection work.

In FY 2018, the EAC was appropriated $380 million for election security grants, and while it is likely that the final FY 2020 funding vehicle includes finds for this program, it is likely to be below $600 million.

Stanford Election Security Report

In standing up its new Cyber Policy Center, Stanford University released a report "Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Elections and Beyond," an attempt to partially produce a commission-style report along the lines of the National Commission on Terrorist Attacks Upon the United States' report on the September 11, 2001 attacks. The report contains detailed recommendations on how the U.S. should defend itself from further Russian attacks in upcoming elections and from other adversaries. Harvard University's Belfer Center for Science and International Affairs launched the Defending Digital Democracy initiative in 2017 that has produced cybersecurity how-to guides for campaigns and governments conducting elections.

As former U.S. Ambassador to Russia Michael McFaul wrote in the Preface "[i]n 2016, Russia attacked the United States." He explained

> More precisely, Russian President Vladimir Putin, his government, and his proxies deployed multiple strategies and instruments—media, doxing, covert operations, direct contacts with Trump associates, and cyber-attacks on U.S. electoral infrastructure—to influence the outcome of the 2016 U.S. presidential election, and more generally, to disrupt the electoral process. Although the Kremlin had intervened previously in the electoral processes of other countries and dabbled in influencing earlier American elections, the scale, scope, and sophistication of this Russian intervention in this American election were unprecedented.

McFaul stated that "the Mueller report lacks comprehensive policy recommendations for how to prevent foreign interventions in future U.S. elections…[and] [a]s discussed throughout this report, the executive branch has implemented several reforms to reduce the threat of foreign meddling in elections." He added that "[t]he U.S. Congress also has proposed several new bills to help the effort, many of which we endorse in this study…[b]ut the response so far does not meet the threat, which as FBI Director Christopher Wray warned in April 2019, remains very real."

The authors made the following recommendations:

Increase the Security of the U.S. Election Infrastructure

2.1. Require that all vote-counting systems provide a voter-verified paper audit trail.
2.2. Require risk-limited auditing for all elections.
2.3. Assess the security of computerized election-related systems in an adversarial manner.
2.4. Establish basic norms regarding digital behavior for campaign officials.
2.5. Commit regular funding streams to strengthen the cybersecurity posture of the election infrastructure.
2.6. Retain the designation of election infrastructure as critical infrastructure.
2.7. Allow political parties to provide cybersecurity assistance to state parties and to individuals running for federal office and their campaigns.

Regulate Online Political Advertising by Foreign Governments and Nationals

3.1. Explicitly prohibit foreign governments and individuals from purchasing online advertisements targeting the American electorate and aimed at influencing U.S. elections.
3.2. Support the passage of the Honest Ads Act with several key amendments.
3.3. Strengthen self-regulation mechanisms for the major internet platforms.

Confront Efforts at Election Manipulation from Foreign Media Organizations

4.1. Require greater disclosure measures for FARA-registered foreign media organizations.
4.2. Mandate additional disclosure measures during pre-election periods.
4.3. Support existing disclosure measures of specific social media platforms.

Combat State-Sponsored Disinformation Campaigns from State-aligned Actors

5.1. Create standardized guidelines for labeling content affiliated with disinformation campaign producers.
5.2. Create norms for the media's handling of stolen information.
5.3. Limit the targeting capabilities for political advertising.
5.4. Expand transparency for paid and unpaid political content.
5.5. Improve the quality and scope of detection tools and reporting policies for social media platforms.
5.6. Build an industry-wide coalition to coordinate and encourage the spread of best practices.
5.7. Remove barriers to the sharing of information relating to disinformation, including changes to privacy and other laws as necessary.
5.8. Establish a Social Media ISAC/ISAO to improve communication between the U.S. government and social media companies about disinformation operations.
5.9. Increase overall transparency on social media platforms.
5.10. Carefully balance platform responsibility with individual freedoms.
5.11. Establish a norm among candidates to not use stolen data or manipulated content.
5.12. Emphasize digital literacy in educational curricula and focus public education on the knowledge that makes democracy more resilient to disinformation campaigns.

Enhance Transparency about Foreign Involvement in U.S. Elections

6.1. Mandate transparency in the use of foreign consultants and foreign companies in U.S. political campaigns.
6.2. Increase transparency about foreign business interests.
6.3. Disclose contacts with foreign nationals and governments.
6.4. Strengthen the norm of one government at a time.

Establish International Norms and Agreements to Prevent Election Interference

7.1. Fortify U.S. and international commitment to human rights.
7.2. Strengthen international norms protecting election infrastructures.
7.3. Create norms to deter the use of disinformation and hacked materials.
7.4. Lead international advocacy against foreign interference through disinformation.
7.5. Distinguish legitimate cross-border assistance from illicit or unlawful interventions.
7.6. Hold congressional hearings about policies to support free and fair elections internationally.
7.7. Promote cooperation among democracies focused on election protection.
7.8. Appoint a senior U.S. government representative on election interference.
7.9. Develop guidelines about platform cooperation with foreign governments.

Deter Foreign Governments from Election Interference

8.1. Recalibrate risk tolerances for actions in cyberspace.
8.2. Signal a clear and credible commitment to respond to election interference.
8.3. Maintain a visible position of U.S. capabilities, intentions, and responses.
8.4. Enact country-specific and timely responses that impose real, effective costs.
8.5. Promote collective engagement with international partners.
8.6. Conduct a continuous strategic disruption campaign against adversaries that seek to interfere with U.S. elections.
8.7. Pursue common interests in cyberspace where possible.

House Judiciary Committee on Antitrust Investigation

A few days after media reports indicated that the U.S. Department of Justice (DOJ) and the Federal Trade Commission (FTC) would be opening antitrust investigations into Google, Amazon, Facebook, and Apple, the House Judiciary Committee announced "a bipartisan investigation into competition in digital markets…[that] will include a series of hearings held by the Subcommittee on Antitrust, Commercial and Administrative Law on the rise of market power online, as well as requests for information that are relevant to the investigation."

The committee stated that "[a] small number of dominant, unregulated platforms have extraordinary power over commerce, communication, and information online…[and] [b]ased on investigative reporting and oversight by international policymakers and enforcers, there are concerns that these platforms have the incentive and ability to harm the competitive process." The committee stated that "[t]he Antitrust Subcommittee will conduct a top-to-bottom review of the market power held by giant tech platforms…[and] [t]his is the first time Congress has undertaken an investigation into this behavior." The committee said the investigation "will focus on three main areas:

- Documenting competition problems in digital markets;
- Examining whether dominant firms are engaging in anti-competitive conduct; and
- Assessing whether existing antitrust laws, competition policies, and current enforcement levels are adequate to address these issues."

However, the Democrats and Republicans' quotes in the press release suggest the leaders on the committee are not entirely aligned. Full Committee Chair Jerrold Nadler (D-NY) said that "there is growing evidence that a handful of gatekeepers have come to capture control over key arteries of online commerce, content, and communications…[and] [g]iven the growing tide of concentration and consolidation across our economy, it is vital that we investigate the current state of competition in digital markets and the health of the antitrust laws." Ranking Member Collins (R-GA) stated that

"[a]s tech has expanded its market share, more and more questions have arisen about whether the market remains competitive…[and] [o]ur bipartisan look at competition in the digital markets gives us the chance to answer these questions and, if necessary, to take action."

Shortly after the investigation was announced, Speaker of the House Nancy Pelosi (D-CA) tweeted

> Unwarranted, concentrated economic power in the hands of a few is dangerous to democracy – especially when digital platforms control content. The era of self-regulation is over.

There were further media reports that the FTC has already requested information from Amazon's competitors on its business practices over the last few months. Reportedly, the FTC has asked for details on three areas:

1) the pricing structure of fulfillment by Amazon, the practice that allows third parties to sell through Amazon
2) Amazon's competition against other sellers in the Amazon Marketplace
3) the bundling of services through Amazon Prime memberships

Yet, just because the FTC is inquiring about some of Amazon's practices does not mean the agency will launch an antitrust action.

Commerce Report on Critical Minerals

Last week, the U.S. Department of Commerce (Commerce) released a report required by an executive order (EO) on critical minerals, many of which are used in technological products commercially and militarily. As explained in the agency's press release, the interagency report was submitted per Executive Order 13817, A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals, and "contains a government-wide action plan, including recommendations to advance research and development efforts, increase domestic activity across the supply chain, streamline permitting, and grow the American critical minerals workforce."

Commerce explained that

> The assured supply of critical minerals and the resiliency of their supply chains are essential to the economic prosperity and national defense of the United States. The United States is heavily dependent on foreign sources of critical minerals and on foreign supply chains resulting in the potential for strategic vulnerabilities to both our economy and military. Mitigating these risks is important and consistent with our country's National Security Strategy and National Defense Strategy to promote American prosperity and to preserve peace through strength.

Commerce added that

> The United States imports most critical mineral commodities. Specifically, the United States is import-reliant (imports are greater than 50 percent of annual consumption) for 31 of the 35 minerals designated as critical by the Department of the Interior. The United States does not have any domestic production and relies completely on imports to supply its demand for 14 critical minerals.

Commerce laid out "6 Calls to Action, 24 goals, and 61 recommendations that describe specific steps that the Federal Government will take to achieve the objectives outlined in Executive Order 13817." Commerce claimed that "[w]hen executed, this strategy will improve the ability of the advanced technology, industrial, and defense manufacturing sectors that use critical minerals to adapt to emerging mineral criticality issues; reduce risks for American businesses that rely on critical minerals; create a favorable U.S. business climate for production facilities at different stages of critical mineral supply chains; and support the economic security and national defense of the United States; all of which will reduce the Nation's vulnerability to critical mineral supply disruptions." Commerce described the Calls to Action:

- **Advance Transformational Research, Development, and Deployment Across Critical Mineral Supply Chains:** Assesses progress toward developing critical minerals recycling and reprocessing technologies, technological alternatives to critical minerals, source diversification, and improving processes for critical mineral extraction, separation, purification, and alloying.
- **Strengthen America's Critical Mineral Supply Chains and Defense Industrial Base:** Discusses ways to improve critical mineral supply chains, which could help reduce risks to U.S. supply by increasing domestic critical mineral resource development, building robust downstream manufacturing capabilities, and ensuring sufficient productive capacity.
- **Enhance International Trade and Cooperation Related to Critical Minerals:** Identifies options for accessing and developing critical minerals through investment and trade with America's allies, discusses areas for international collaboration and cooperation, and ensures robust enforcement of U.S. trade laws and international agreements that help address adverse impacts of market-distorting foreign trade conduct.
- **Improve Understanding of Domestic Critical Mineral Resources:** Provides a plan to: improve and publicize the topographical, geological, geophysical, and bathymetrical mapping of the United States; support mineral information collection and analysis of commodity-specific mitigation strategies; focus and prioritize interagency efforts; and conduct critical mineral resource assessments to support domestic mineral exploration and development of conventional sources (minerals obtained directly through mining an ore), secondary sources (recycled materials, post-industrial, and post-consumer materials), and unconventional sources (minerals obtained from sources such as mine tailings, coal byproducts, extraction from seawater, and geothermal brines) of critical minerals.
- **Improve Access to Domestic Critical Mineral Resources on Federal Lands and Reduce Federal Permitting Timeframes:** Provides recommendations to streamline permitting and review processes related to developing mining claims or leases and enhancing access to domestic critical mineral resources.
- **Grow the American Critical Minerals Workforce:** Discusses the activities related to critical minerals needed to develop and maintain a strong domestic workforce to foster a robust domestic industrial base.

Commerce's report comes at a time when the People's Republic of China (PRC) is threatening to cut off the U.S.'s supply of rare earths as a means of countering U.S. pressure in trade talks, notably by pressing Huawei and ZTE. The PRC currently produces and processes the lion's share of rare earth materials and should the U.S. lose its supply, the supply of consumer goods and high-technology military weapons could be disrupted. In 2010, the PRC announced that it would cut production of rare earths by 72% and actually cut off shipments to Japan over a dispute over which country owns the Senkaku Islands.

In 2016, the Government Accountability Office (GAO) observed that "[t]he Department of Defense (DOD) depends on rare earth materials (rare earths) to provide functionality in weapon systems components." In a 2018 report on the defense industrial base, the DOD acknowledged that rare earths are used in the manufacture of "lasers, radar, sonar, night vision systems, missile guidance, jet engines, and even alloys for armored vehicles."

Federal Data Strategy Released and Input Requested on Action Plan

The Office of Management and Budget (OMB) has released the Administration's Federal Data Strategy, and the Administration has released a draft Action Plan. Last fall, 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 President's Management Agenda (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 ofthe 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.

The place where the Federal Data Strategy may most immediately come into play regarding data security is with the second group of "Practices:" "Governing, Managing, and Protecting Data," which will necessarily bleed over into other federal efforts to protect its information systems and the information they hold, store, and transmit. For example, some of the practices include "Govern Data to Protect Confidentiality and Privacy," "Protect Data Integrity," and "Leverage Data Standards." Last year, the Administration initiated the process of drafting its Practices, which have since been finalized.

In the draft Action Plan, the Administration explained that

> Executive Branch agencies will implement the Strategy in accordance with OMB guidance and by adhering to the requirements of annual Federal Data Strategy Action Plans. These

> plans will identify a subset of action steps related to practices that are the priority for a given year, along with targeted timeframes for implementation and identified actors. This approach allows for continuous innovation with focused, measured progress, along with opportunities to improve and adapt plans for future actions. OMB may assess agencies on their progress in implementing these practices through the Federal Data Strategy Action Plans and any of its existing oversight and coordination mechanisms.

The Administration is asking for "[c]omments specific and responsive to the following are requested:

> 1. Identify additional actions needed to implement the Federal Data Strategy that are not included in the draft Action Plan and explain why.
> 2. Identify additional actions that would align with or complement ongoing Federal data initiatives or the implementation of new legislation, such as the Foundations for Evidence-based Policy Making Act of 2018 and explain why.
> 3. Identify any actions in the draft Action Plan that should be considered for omission and explain why.
> 4. For each action, provide any edits and additional detail to ensure that they accurately and effectively describe needed activities, responsible entities, metrics for assessing progress, and timelines for completion.
> 5. For each action, provide information about the implementation resources necessary to ensure success of the action steps.

Administration Asks Congress To Delay and Soften Huawei and ZTE Ban

The Office of Management and Budget (OMB) sent a request to Congress on June 4 to change provisions in in the FY 2019 National Defense Authorization Act (NDAA) that would change provisions banning the federal government from using Huawei or ZTE or doing business with contractors that have either Chinese firms' parts or components in their systems or supply chains. The Administration is asking to soften the language and impact and delay implementation of Section 889, the provisions aimed at barring contractors and federal agencies from using Huawei and ZTE products, equipment, and services. Moreover, OMB is asking that Congress include proposed legislative language into the FY 2020 NDAA.

OMB is asking for significant legislative changes. The Administration is asking to delay the effective date for the language barring virtually all federal agencies from entering into contracts with entities that use "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." This prohibition would be delayed from taking effect from in August 2020 until August 2022. Likewise, the language barring the issuance of federal grants or loans to such entities would also be delayed until August 2022. Additionally, the ban on the use of federal loans and grants would no longer be applied to the agencies themselves; rather, it would the recipients of the grants and loans (e.g. a state or city) that would have the obligation not to buy or contract for services or products that would run afoul of the de facto ban on Huawei and ZTE.

The Federal Acquisition Regulatory Council would be tasked with a rulemaking to address the problems posed by (a)(1)(b) (i.e. the language barring a federal agency from contracting with any entity with any ZTE or Huawei components or equipment) including two public meetings. Last week, the Department of Defense (DOD), the General Services Administration (GSA), and the National

Aeronautics and Space Administration (NASA) announced a meeting "to obtain views of experts and interested parties regarding implementation of section 889 of Title VII of the NDAA for FY 2019." This public meeting will focus on one provision in Section 889 ((a)(1)(B)), the language that "prohibits agencies from entering into a contract (or extending or renewing a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." Under the Administration's request, OMB would also need to solicit public feedback in how to implement the provisions on federal grants and loans.

Notably, OMB is not seeking changes to the ban preventing agencies from "procur[ing] or obtain[ing] or extend[ing] or renew[ing] a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." This provision of Section 889 (i.e. (a)(1)(A)) is subject to a rulemaking under FAR Case 2018-017, and, as of yet, a notice of proposed rulemaking has not yet been released.

In terms of the policy rationale for requesting the changes, OMB stated that "[w]hile the Administration recognizes the importance of these prohibitions to national security, a number of agencies have heard significant concerns from a wide range of potentially impacted stakeholders who would be affected by section 889, which the Administration believes could be addressed with a modified implementation schedule." OMB claimed that "[c]hallenges that could arise under the current schedule potentially include a dramatic reduction in the available industrial base (including small business suppliers), who will no longer be able to sell to the Government, either because their non-government business is more valuable, or due to the cost of the potential regulatory burdens associated with compliance with subsections (a)(1)(B) and (b)(1)." OMB added that "rural Federal grants recipients may be disproportionally impacted by the prohibition from using Federal funds to enter into contracts with entities that use covered telecommunications equipment or services due to the limited number of market options in rural areas."

Further Reading

"The EU's Embassy In Russia Was Hacked But The EU Kept It A Secret" – *BuzzFeed News*
"YouTube's purge of white supremacist videos also hits anti-racism channels" – *The Los Angeles Times*
"Explainer: Should Big Tech fear U.S. antitrust enforcers?" – *Reuters*
"Democratic Candidates Woo Silicon Valley for Donations, Then Bash It" – *The New York Times*
"Tech Giants Amass a Lobbying Army for an Epic Washington Battle" – *The New York Times*
"Russia says Tinder must share user data, private messages" – *ZDNet*