Michael Kans' Technology Policy Update
28 August 2019
By Michael Kans, Esq.

Spotlight: A Privacy Bill A Week

As we wait for stakeholders in Congress to finalize and release their proposals to regulate how private sector companies handle, use, and distribute the private information of Americans, we thought there would be value in reviewing some of the key bills already introduced this Congress and some introduced over the last few Congresses so when bills are finally introduced, we will have a baseline by which to judge the proposal.

This week, let's examine the "Data Care Act" (S. 3744). In December 2018, fifteen Democratic Senators led by Senator Brian Schatz (D-HI) introduced a bill that would extend the concept of fiduciary responsibility currently binding on health care professionals and attorneys with respect to the patients and clients' information to "online service providers". In short, under the "Data Care Act," online service providers would be severely be limited on how they collect, share, and sell the personally identifiable information (PII), for these companies would need to treat their customers' PII as privileged and deserving of a greater level of protection, much like the HIPAA regulations impose this standard on health care providers or bar associations' rules on attorneys. However, the scope of who is an online service provider would seem to encompass most consumer-oriented companies doing business on the internet. Yet, like most other privacy and data security bills, the Federal Trade Commission (FTC) would enforce the new regime.

An "online service provider" is defined as an entity "engaged in interstate commerce over the internet or any other digital network; and in the course of business, collects individual identifying data about end users, including in a manner that is incidental to the business conducted." This very sweeping definition would cover almost any business or entity doing business in the U.S. even if it is not across state lines as the Supreme Court has often construed the Commerce Clause. However, the FTC would have the discretionary authority to exclude categories of online service providers from the fiduciary duties the bill would otherwise impose. The FTC is directed to consider the privacy risks posed by the category of online service provider.

The bill requires that "[a]n online service provider shall fulfill the duties of care, loyalty, and confidentiality" towards consumers' personal information, which is also broadly defined in the bill. The duty of care requires online service providers to "reasonably" safeguard "individual identifying data" from unauthorized access and notify consumers of any breach of this duty, subject to FTC regulations that would be promulgated. The duty of loyalty would require online service providers to not use the information in a way that benefits them to the detriment of consumers, including uses that would result in reasonably foreseeable material physical or financial harm to the consumer. Finally, the duty of confidentiality limits the disclosure or sale of consumers' information to instances where the duties of care and loyalty are observed (i.e. when the information must be safeguarded and not used to the detriment of consumers). Moreover, under this duty, should an online service provider wish to share or sell consumers' information with a third party, they would need to enter into a contract with the other party that requires them to meet the same duties of care, loyalty, and confidentiality.

As noted, the FTC would enforce the Act and would have the authority to levy fines in the first instance for violations, but state attorneys general would also be able to bring actions for violations in the event the FTC does not act or after FTC action. This latter power has long been a Democratic priority in the realm of data security and may be a non-starter with Republicans. Moreover, the bill does not preempt state laws, meaning the FTC could investigate a violation under this act and states could investigate under their laws. The FTC would be given authority under the Administrative Procedure Act (APA) to promulgate regulations regarding data breach notification instead of the much more onerous Moss-Magnuson rulemaking procedures the FTC must otherwise use. These regulations include the aforementioned regulations on breach notification and some possible exemptions to the duties that would otherwise apply to online service providers (e.g. small companies). The bill expands the FTC's jurisdiction over non-profit entities and common carriers that may also be online service providers.

OMB Finally Submits FY 2018 FISMA Report

The Office of Budget and Management (OMB) has finally released the FY 2018 Federal Information Security Modernization Act (FISMA) report to Congress, an annual report that FISMA requires the Administration to submit by March 1. Overall, federal civilian agencies reported 12% fewer incidents than FY 2017, and this marks the first year there were no "major incidents" reported. However, much of the report reiterates previously announced and ongoing initiatives, containing little new information on these initiatives. Nonetheless, the report does provide data on civilian agency cybersecurity and FISMA compliance.

OMB asserted that there were "31,107 incidents reported by Federal agencies, and validated with US- CERT, across nine attack vector categories...[and] [t]his represents a 12% decrease from FY 2017, when agencies reported 35,277 incidents." OMB acknowledged that "[w]hile the trend is encouraging, drawing conclusions based on this data point, particularly as agencies have adjusted to several new sets of reporting guidelines over the last few years, would be concerning." OMB added that "email-based threats remain prevalent, with Email/Phishing continuing to be a highly-targeted attack vector...[and] [a]ccording to information provided by DHS, 6,930 incidents occurring in the past year." OMB stated that "nearly 27% of all incidents did not have an identified attack vector, which continues to suggest that the government must take additional steps to help agencies identify the sources and vectors of these incidents."

OMB touted that agencies did not report any “major incidents,” a term that has undergone frequent redefinition over the last few years. OMB’s latest redefinition of a “major incident” is either:

> I. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Agencies should determine the level of impact of the incident by using the existing incident management process established in National Institute of Standards and Technology (NIST)Special Publication (SP) 800-61, Computer Security Incident Handling Guide.
>
> OR,
>
> II. A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

As noted earlier, "Section I: Federal Cybersecurity Activities," largely rehashes initiatives and developments launched in FY 2018 and earlier with little in the way of updates on how the Administration is progressing on these measures. OMB focused on two deliverables from Executive Order 13800 that underpinned cybersecurity efforts in FY 2018:

- The Report to the President on Federal IT Modernization, details activities to modernize and safeguard high-risk High Value Assets (HVAs), promotes the consolidation of network acquisitions and management, and prompts agencies to leverage commercial cloud solutions and cybersecurity shared services where available.
- The second deliverable, the Federal Cybersecurity Risk Determination Report and Action Plan, assesses the state of agencies' cybersecurity risk management efforts and includes a plan for addressing these areas of risks. The four core actions identified for reducing cybersecurity risk were: (1) Increasing cybersecurity threat awareness; (2) Standardizing cybersecurity and IT capabilities; (3) Maturing Security Operations Centers (SOCs); and (4) Driving agency accountability.

OMB stated that "[t]hroughout 2018, OMB, [the Department of Homeland Security], and the broader Federal IT and cybersecurity community have taken concrete steps toward achieving these actions." The following excerpts stand as the only narrative in the report on how the Administration progressed on these initiatives:

- During FY 2018, the Continuing Diagnostics and Mitigation (CDM) program office also successfully established data exchanges between all 23 civilian CFO Act agency dashboards and the Federal dashboard, which is hosted at the DHS National Cybersecurity and Communications Integration Center (NCCIC). Additionally, the CDM program office connected almost a dozen non-CFO Act agencies to the CDM Shared Services Platform and worked to onboard more than 40 additional non-CFO Act agencies. Furthermore, the CDM program office has made Phase 3 boundary protection, event management, and security lifecycle tools available to 96% of participating agencies through the CDM DEFEND contract.
- In FY 2018, DHS conducted 61 High Value Asset (HVA) assessments, resulting in 356 findings (221 System Architecture Review findings and 135 Risk and Vulnerability Assessment findings). These assessments revealed that the Federal Government's continues to face challenges mitigating basic security vulnerabilities.
- As part of the updated Trusted Internet Connections (TIC) initiative, expected to be released in FY 2019, DHS will define TIC initiative requirements in documentation called TIC Use Cases. The TIC Use Case documentation will outline which alternative security controls, such as endpoint and user- based protections, must be in place for specific use cases where traffic is not required to flow through a physical TIC access point. Agencies are required to meet the requirements detailed in the TIC Use Cases guidance.

OMB did provide a number of overviews of agency cybersecurity operations and included these figures on unclassified cybersecurity funding in FY 2018 which necessarily exclude most of the Department of Defense and Intelligence Community's spend:

Table 2 FY 2018 Cybersecurity Spending

Agency	FY 2018 Spend ($ Millions)	Agency	FY 2018 Spend ($ Millions)
Commerce	$349.7	NASA	$170.7
DHS	$1,858.9	NRC	$24.6
DOD	$8,048.0	NSF	$246.7
DOT	$184.8	OPM	$38.5
ED	$103.8	SBA	$9.1
Energy	$447.9	SSA	$167.1
EPA	$21.1	State	$361.5
GSA	$71.6	Treasury	$445.3
HHS	$359.0	USAID	$43.8
HUD	$14.9	USDA	$261.7
Interior	$87.9	VA	$385.9
Justice	$820.8	Non-CFO Act	$361.8
Labor	$92.9		
		Total	**$14,978**

In Section III: Agency Performance, each civilian agency is assessed according to its implementation of the Cybersecurity Framework, CIO Rating, CIO Self-Assessment, Independent Assessment, and a count of US-CERT incidents by attack vector. This is mostly new information, much of which came from the inspectors general' annual FISMA assessments.

OMB was months late in submitting this report to Congress. Last month, when the Government Accountability Office (GAO) was investigating federal information security and asked when OMB would submit its FY 2018 FISMA report, OMB claimed the FISMA report was five months late because of the 35-day government shutdown earlier this year. Moreover, OMB could not commit to a date as to when this statutorily required report would be submitted to Congress.

NTIA To Hold Software Component Meeting

The Department of Commerce's National Telecommunications Information Administration (NTIA) will hold another public meeting in its multistakeholder process on promoting software component transparency on September 5, 2019. NTIA explained "[t]he main objectives of the meeting are to review drafts provided by the working groups, discuss how they complement each other, and hear feedback from the broader stakeholder community." NTIA stated that "[s]takeholders will also identify next steps in this effort, how progress can be made on extending the basic model, collecting tooling, and promoting awareness and adoption of stakeholder work." This NTIA multistakeholder, voluntary process centers on the idea that all parties developing and using software should be able to trace the origin and development of any software. Consequently, problems, weaknesses, and vulnerabilities would be much easier to locate, track, and ideally eliminate.

This initiative grew out of previous NTIA multistakeholder processes on "information and cyber policy and security, the Internet of Things (IoT), and the health of the digital ecosystem" dating back to the Obama Administration. The most recent stakeholder process that informs the software component transparency initiative was the request for comments that was used to draft "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats." In the June 2018 Federal Register notice announcing this initiative, NTIA asserted that "[t]he goal of this initiative is to foster a market that offers greater transparency on software components." NTIA added that "[s]takeholders will engage in an open and transparent process to explore the benefits and any potential risks of greater transparency...[and] [t]hey may focus on incentives and barriers to adoption of transparency practices...[which] could include policy and international components." NTIA stated that "[t]ransparency-driven solutions need not be prescriptive or regulatory, and can accommodate an ecosystem without a one-size-fits-all approach." NTIA further explained "[t]he importance of transparency in information security is widely recognized, and the notion of transparency around components of software and connected devices is not new. Academics identified the potential value of a "software bill of materials" as far back as 1995, and there are a growing number of commercial solutions for security, licensing, and asset management."

As noted, this meeting is not the first, and the work at the last meeting will serve at the foundation for this meeting. At the June 27 meeting, the NTIA and its partners discussed the following documents:

- Framing WG: Framing Software Component Transparency
- Use Cases WG: SBoM Roles and Benefits
- Formats WG: Draft White Paper
- Healthcare PoC: Read-ahead Summary of PoC Exercise
- Framing WG Presentation
- Use Cases WG Presentation
- Formats WG Presentation
- Healthcare PoC Presentation

It is likely stakeholders will update, develop, and revise these documents and then circulate new drafts and documents for consideration.

At the end of the day, a multistakeholder process with the imprimatur of NTIA will carry weight in policy circles and will inform the thinking of policy and lawmakers. Whether legislation, executive action, or a defacto standard on a software bill of goods results is not knowable at this point. Considering that the origin and development of software is akin to the origin of components in a technology company's supply chain, it is very likely this is a facet of securing U.S. systems and networks that will receive increased attention in Washington.

CISA Articulates Its Strategic Intent

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has released a "Strategic Intent" document that "lays out the strategic vision and operational priorities of the CISA Director" Christopher Krebs and provides top-level direction to CISA. Of course, CISA came into being in November 2018 with the enactment of legislation renaming and reorganizing the National Protection and Programs Directorate (NPPD) and grouping other DHS components into this new entity. CISA assumed of all NPPD's cybersecurity and infrastructure

responsibilities and received some new authority under the enabling statute to make the agency the locus in the federal government for most public and private sector cybersecurity issues.

Not surprisingly, CISA is still in the process of undertaking a number of foundational activities such as laying out its strategic vision. For example, in late April, CISA released the new "National Critical Functions" that will reorient the federal government's view on risks to U.S. critical infrastructure holistically instead of the approach relying on a sector-specific regime, including cyberecurity. "Strategic Intent" will serve CISA until a long-term strategic plan is drafted, but the agency did not provide a timeline as to when this would occur. And yet, the Strategic Intent does identify Krebs' top five priorities that cut across the agency's articulated goals and objectives: 1) China, Supply Chain, and 5G; 2) Election Security; 3) Soft Target Security; 4) Federal Cybersecurity; and 5) Industrial Control Systems, and CISA has already been addressing some of these issues through working groups and the use of authority to issue directives.

CISA explained that the document "provides a general approach for how we execute our responsibilities and serves as a reference point for our employees and partners to guide our work and create unity of effort...[and] aims to position us to successfully meet our mission in the coming years and decades. It serves as the interim strategy as we develop a longer-term strategic plan." The agency claimed that "[t]he common framework of goals and outcomes helps organize our mission execution and inform management decisions—including operations planning, requirements generation, budget formulation, and performance management." CISA acknowledged that "[t]hese are high-level outcomes that we will constantly seek to achieve; specific actions and milestones will appear in operational and organizational plans...[and] [t]hese goals and outcomes give us a constant foundation for capability and direction as threats and the mission space dramatically evolve."

Krebs listed his five "Operational Priorities" after noting that "[w]hile the goals and outcomes within of the Strategic Intent create a common framework across our entire mission space and activities, the Director has five specific operational areas of focus that, in some cases, span across several goals and objectives:"

> 1. CHINA, SUPPLY CHAIN, AND 5G. China presents the most pressing long-term strategic risk to the United States. The persistent threat posed by China compels CISA's focus on supply chain risk management in the context of national security. CISA is looking to reduce the risks of Chinese supply chain compromise, whether that is through 5G or any other technologies.
> 2. ELECTION SECURITY. CISA is responsible for assisting state and local governments, and the private sector organizations that support them, with their efforts to enhance the security and resilience of election infrastructure. CISA's objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, which are essential to the conduct of free and fair democratic elections. We will pivot off the trust, expertise, and relationships developed through our election security work to broaden our State and Local cybersecurity risk management efforts.
> 3. SOFT TARGET SECURITY. Intentional targeting of soft targets and crowded places presents a daunting security challenge—undermining traditional risk management and physical security practices by deliberately exploiting vulnerabilities. As the DHS lead for the soft targets and crowded places security effort, CISA supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country's economy.

4. FEDERAL CYBERSECURITY. The speed of change in the cyber world is outpacing the current federal "policy to implementation" process. CISA leads the Federal Government in confronting this challenge with a unity of purpose that drives federal agencies to make risk-informed cybersecurity decisions. CISA's authorities present the capability and opportunity to create federal cybersecurity approaches that address the speed of change. We will also use our insight, expertise, capabilities and reach to assist our State and Local government partners in improving their cybersecurity posture and defending against the outbreak of ransomware.

5. INDUSTRIAL CONTROL SYSTEMS. Much of critical infrastructure shares a common characteristic: a dependence on industrial control systems (ICS). ICS control, monitor, and manage essential functions for a wide array of critical infrastructure, including transportation systems, telecommunications networks, industrial manufacturing plants, electric power generators, oil and natural gas pipelines, and more recently, the Internet of Things. CISA leads the Federal Government's unified effort to work with the ICS community to reduce risk to our critical infrastructure by strengthening control systems' security and resilience.

CISA stated its broader goals and the objectives it hopes to achieve:

- GOAL 1: DEFEND TODAY
  - OBJECTIVE 1.1. CYBER DEFENSE. Significant cyber threats are unable to achieve their objectives in CISA mission space.
  - OBJECTIVE 1.2. PHYSICAL HAZARDS. Impacts from physical hazards are minimized through coordinated incident preparation and response.
  - OBJECTIVE 1.3. INCIDENT COMMUNICATIONS. Voice, video, and data communications are available and interoperable during daily operations and incident response.
  - OBJECTIVE 1.4. HYBRID, SUPPLY CHAIN, AND EMERGING THREATS. Hybrid, supply chain, and emerging threats are unable to achieve their objectives in CISA mission space.
- GOAL 2: SECURE TOMORROW
  - OBJECTIVE 2.1. CRITICAL INFRASTRUCTURE RESILIENCE AND CAPACITY BUILDING. The community maintains an appropriate level of security and resilience through risk management and capacity building.
  - OBJECTIVE 2.2. FEDERAL CYBER- SECURITY GOVERNANCE AND CAPACITY BUILDING. Cybersecurity risk in federal civilian executive branch agencies is managed at an acceptable level, commensurate with each agency's own risk and that of the broader federal enterprise.
  - OBJECTIVE 2.3. EMERGENCY COMMUNICATIONS GOVERNANCE AND CAPACITY BUILDING. Responders at all levels of government have the ability to seamlessly share voice, video, and data communications during daily operations and major incidents and events.
  - OBJECTIVE 2.4. LONG-TERM RISK MANAGEMENT. Long-term risks are addressed through collaborative risk management across the community.
- GOAL 3: MISSION SUPPORT
  - OBJECTIVE 3.1. WORKFORCE DEVELOPMENT AND RETENTION. Missions and mission support are fully staffed with the appropriate skills, competencies, and performance. The CISA workforce directly reflects the strengths and vibrancy of a diverse and inclusive Nation and, to a person, is provided an equal opportunity to thrive.

- OBJECTIVE 3.2. TRANSFORMATION. CISA successfully designs, validates, and implements the CISA 2020 internal change management campaign to unify the agency, enhance mission effectiveness, and improve the overall CISA employee experience.
- OBJECTIVE 3.3. CAPABILITY DELIVERY. Mission operators and partners receive new capabilities in a timely and effective manner to address evolving threats.
- OBJECTIVE 3.4. MISSION SUPPORT MANAGEMENT. CISA exceeds Federal Government averages on mission support performance.

A DHS Advisory Committee To Consider Recommendations on ICT Supply Chain Issues

A Department of Homeland Security advisory committee announced a meeting early next month to consider, among other items, a draft report on "technology capabilities that are critical to national security and emergency preparedness (NS/EP) functions in the evolving Information and Communications Technology (ICT) ecosystem, and Government measures and policy actions to manage near term risks, support innovation, and enhance vendor diversity for NS/EP critical capabilities." This report is part of the response by the Trump Administration to the threats created by a global supply chain for the ICT industry that includes China, and it contains recommendations to address the risks inherent in such a supply chain. The National Security Council's Senior Director for Cybersecurity Policy Grant Schneider and CISA Cybersecurity Division Director Jeanette Manfra will both make remarks at this meeting which will be held by conference call on September 3, 2019.

The President's National Security Telecommunications Advisory Committee (NSTAC) is housed with the Cybersecurity and Infrastructure Security Agency (CISA) at DHS and consists almost exclusively of private sector individuals representing companies like AT&T, Microsoft, Raytheon, Avaya, Oracle, and others. NSTAC has weighed in on a number of technology, emergency, and national security issues over the last few years (e.g. big data analytics in 2016, internet and communications resilience in 2017, and on a "cyber moonshot" last year.) NSTAC will consider the draft report titled "NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem," and NSTAC's deliberations and final report are part of the Trump Administration's larger efforts to address issues raised by the supply chain of technologies companies that includes Chinese made products and companies like Huawei. For example, in May 2019, the White House issued Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain." Also, the DHS National Risk Management Center (NMRC) is developing its own recommendations to the White House on how the U.S. should address supply chain issues. Additionally, there are executive branch actions underway as a result of enacted legislation such as the newly formed Federal Acquisition Supply Chain Security Council, and the interim rule issued this month barring federal agencies from buying Huawei, ZTE, and other Chinese companies' products.

NSTAC explained that the White House tasked it with examining "technology capabilities that are critical to NS/EP functions in the evolving ICT ecosystem" in August 2018. This study was to be divided into two phases: "current technology capabilities across the ICT ecosystem that are most critical to the Government's NS/EP functions in the next five to ten years...[and] [i]n a letter to the President dated April 2, 2019, the NSTAC completed the first phase and identified three representative technologies highly critical to the U.S. NS/EP mission: 5G wireless technology; quantum computing; and AI/ML." NSTAC stated that second phase "required the NSTAC to make recommendations for enhancing resiliency and fostering innovation, and this report does so with consideration of the technologies identified in phase one."

NSTAC expressed its belief that "U.S. Government efforts should encourage the availability, evolution, and use of trusted technologies, particularly for those sectors/companies which directly or indirectly support NS/EP missions." NSTAC stated that "[t]here must be a stronger national commitment to creating and preserving vibrant, diverse, and trusted supply chains for NS/EP technology, and stronger central coordination of all U.S. Government efforts toward that end." NSTAC stated that "[t]he United States requires a holistic national strategy and a dedicated White House position to coordinate the development and implementation of that strategy across U.S. departments and agencies (D/As) (especially the national security community), the critical infrastructure provider community, and the innovation community."

To these ends, NSTAC recommended that the President:

- Create, by issuance of an EO, the position of a new Senior Advisor to the President for ICT Resiliency.
- Empower the Senior Advisor to lead the interagency development and implementation of a national policy and Strategy on advancing ICT resiliency and fostering innovation in close coordination with the National Security Advisor, the Director of the National Economic Council (NEC), the Director of Office of Science and Technology Policy (OSTP), the heads of the relevant D/As, and relevant private sector stakeholders. The central goal of the Strategy will be to ensure vibrant, diverse, and trusted supply chains for NS/EP-critical ICT, and to promote competition to that end. The NSTAC recommends many goals and sub-goals be considered for inclusion in the Strategy, [including]:

    1. Identify the stakeholders critical to achieving the resiliency and innovation goals outlined in the Strategy. Recommend specific mechanisms by which the U.S. Government can help foster idea and information exchange, as well as policy coordination and collaboration, amongst key stakeholders. Much of the change that needs to happen involves private sector action, reinforced where appropriate by Government.
    2. Create a multi-stakeholder process to solicit recommendations from the identified stakeholders to advance the resiliency of NS/EP-critical ICT.
    3. Identify gaps in policy, budget, and authorities that hamper the achievement of the Strategy's goals and develop and implement a plan for closing those gaps, including granting new authorities where necessary.
    4. Identify and leverage the U.S.' natural strategic advantages in order to seek to leverage, to the maximum extent, the aspects of the U.S. society and economy that confer advantages upon the Nation as the United States seeks to maintain its global preeminence in innovation.
    5. Foster stronger cooperation amongst like-minded nations to ensure vibrant, diverse, and trusted global supply chains for ICT products. Given the interconnectedness of networks, the challenge of ICT security and resiliency is an international issue, and it is impossible to address the roots or the impacts of this problem from a U.S.-only perspective. The United States must consider what international fora and bodies facilitate international dialogue and engagement on ICT security and resiliency and seek to augment this dialogue and engagement.
    6. Verify that the U.S. Government utilizes its authorities and capabilities to ensure that it is properly aligned and resourced to support the achievement of the overarching goal and sub-goals of the Strategy. Ensure that those authorities and capabilities are well-coordinated, and objectives are achieved efficiently.

NSTAC described its ultimate goals as its "Desired End State:"

- Those responsible for NS/EP missions must have vibrant and diverse choices of trusted technologies and technology providers.
- The U.S. Government must coordinate closely with industry to identify trends that threaten the security and resiliency of the supply chains for ICT technology that enable and support (or will enable and support) NS/EP functions.
- The U.S. Government must foster the conditions that sustain key manufacturing capabilities and capacity in the face of unfair foreign support and to keep the United States on the forefront of innovation, to the greatest extent possible, in strategically important areas of technology.
- The U.S. Government must help industries that are, or will be, critical to U.S. NS/EP to be successful, and to ensure policies that are harmful to them are minimized.

As always, it remains to be seen which recommendations the Administrations accepts and of those which are implemented and to what degree. For example, this new Senior Advisor to the President for ICT Resiliency would need to navigate the various government departments and agencies currently charged with regulating or overseeing the ICT supply chain, and this may prove so difficult that any proposed policies are not fully implemented. Additionally, in the current White House, a well-developed policy crafted with the input and acceptance of various stakeholders could discarded or partially implemented at the whim of the President and other top advisors. While this is a significant, serious effort to address ICT issues, it is not clear how many of these recommendations are acted upon and what effect they may have.

Interim Rule Banning Huawei and ZTE Issued

As required by Section 889 of the FY 2019 National Defense Authorization Act (NDAA) (P.L. 115-232), the Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) have released an interim rule that bars federal agencies from buying Huawei, ZTE, and related Chinese "equipment, system[s], or service[s] 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" unless an exception allows the agency to disregard this general ban. This rule took effect on August 13 per the deadline set in the FY 2019 NDAA. It bears note that this interim rule is applicable to all contracts going forward and some solicitations offered and contracts signed before August 13. The agencies are accepting comments on this interim rule until October 5, 2019 that will be used to formulate a final rule.

However, this rulemaking is but one part of implementing Section 889 (i.e. (a)(1)(A)), and the agencies must put into effect the other operative language by August 13, 2020, presumably via another amendment to the Federal Acquisition Regulations (FAR). Section 889 (a)(1)(B) bars all federal agencies from "enter[ing] into a contract (or extend or renew 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." And, (a)(2) bars the use of federal grants or loans for buying covered telecommunications equipment, systems, or services.

As mentioned earlier, under this interim rule, generally agencies cannot buy Huawei, ZTE, or other related Chinese equipment, systems, or services subject to the exception that the rule "does not prohibit agencies from procuring or contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

However, heads of agencies may grant one-time waivers "to a Government-entity" to buy prohibited equipment, systems, and services if there is "[a] compelling justification for the additional time to implement the requirements...as determined by the head of the executive agency." The government-entity requesting the waiver must also provide "[a] full and complete laydown or description of the presences of covered telecommunications or video surveillance equipment or services in the relevant supply chain and a phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from the relevant systems." If a waiver is granted, Congress must be provided the laydown of covered telecommunications, and the waiver is only good until August 13, 2021 with no extensions being possible. Additionally, the Director of National Intelligence (DNI) may grant a waiver if it serves the interest of national security.

However, the use of this waiver authority does not seem entirely clear. Does the Department of the Army count as a "government-entity"? If so, is the entire service is limited to one waiver? Or is it each component of the Army? Or each contracting office or requirements office, as suggested by the text of the rule? If the latter, the Secretary of the Army could be presented with many such waiver requests. This ambiguity may possibly be addressed in the final rule or perhaps the agencies prefer the flexibility this opacity provides. Additionally, the DNI's authority to grant waivers doesn't seem entirely clear either. Is it just for Intelligence Community (IC) agencies or across the federal government. Moreover, could a government-entity turned down by its agency head essentially appeal this denial by requesting a waiver from the DNI on national security grounds?

There are some pre-August 13, 2019 solicitations and contracts that will be subject to this new interim rule. The agencies explained the applicability of the interim rule for federal contracts as follows:

- Contracting officers shall include the provision at FAR 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment and clause at FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment as prescribed—
    - In solicitations issued on or after August 13, 2019, and resultant contracts; and
    - In solicitations issued before August 13, 2019, provided award of the resulting contract(s) occurs on or after August 13, 2019.
- Contracting officers shall modify, in accordance with FAR 1.108(d), existing indefinite delivery contracts to include the FAR clause for future orders, prior to placing any future orders.
- If modifying an existing contract or task or delivery order to extend the period of performance, including exercising an option, contracting officers shall include the clause in accordance with 1.108(d).
- The contracting officer shall include the provision at 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, in all solicitations for an order, or notices of intent to place an order, including those issued before August 13, 2019, where performance will occur on or after that date, under an existing indefinite delivery contract.

The agencies addressed issues in this rule Congress was silent on: are acquisitions below the simplified acquisition threshold (SAT) subject to the rule? Also, are commercially available off-the-shelf (COTS) items subject to the rule? The answer to both questions is yes. The agencies noted

> The FAR Council has determined that it is in the best interest of the Government to apply the rule to contracts at or below the SAT and for the acquisition of commercial items. The Administrator for Federal Procurement Policy has determined that it is in the best interest of the Government to apply this rule to contracts for the acquisition of COTS items.

Finally, as part of the new language in the FAR, contractors will need to affirmatively inform the agency whether they have any covered telecommunications. The regulations provide the party offering the equipment, systems, or services must indicate whether it "will or will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation." This is very broad as it covers not just the immediate contract but also any subsequent subcontracts and "other contractual instrument resulting from this solicitation." This would suggest an ongoing duty for any prime contractor to monitor its subcontractors or any other contracts related to the government contract to ensure that no one is using "covered telecommunications equipment." In fact, the agencies stated the "clause at FAR 52.204-25 requires contractors and subcontractors to report to the contracting officer, or for DoD through https://dibnet.dod.mil, any discovery of covered telecommunications equipment or services during the course of contract performance." And, if a contractor says that it has covered telecommunications equipment, systems, or services in the first instance, "the offeror is required to further disclose substantial detail regarding the basis for the affirmative representation."

As noted earlier, the Section 889 language that bars entities using Huawei or ZTE equipment, systems, or services takes effect in one year, most likely meaning that next summer the agencies will issue a regulation. Yet, it is not knowable whether the agencies will again issue an interim rule with an immediate effective date or a notice of proposed rulemaking. The Administration requested that Congress change other language in the bill set to also take effect on August 13, 2020: a prohibition for those entities receiving federal grants or loans to use these funds to buy Huawei or ZTE equipment, systems, or services.

In a letter, the Office of Management and Budget (OMB) asked Congress for legislative changes to the grant and loan language and to push back the deadline for both of these provisions from August 13, 2020 to August 13, 2022. None of this language was inserted in either the House or Senate FY 2020 NDAA, and in a demonstration of the receptivity on the Hill to the Administration's request, the House Armed Services Committee included language in its FY 2020 NDAA further tightening the Huawei/ZTE ban for "for the procurement of telecommunications services or installations of telecommunications infrastructure on national security installations located on territories of the United States in the Pacific Ocean unless the contractor is American-owned or American-operated" (i.e. no relation to Huawei or ZTE).

This rulemaking is playing out during an escalating trade war between China and The U.S. spurred, in part, on Huawei's increasing dominance of some sectors of the technology field and concerns about Chinese efforts to dominate the semi-conductor, artificial intelligence, and machine-learning fields. The White House has issued a number of executive orders to change relevant U.S. policy and has launched a number of initiatives. Notably, in May 2019, the Administration issued Executive

Order 13873, Securing the Information and Communications Technology and Services Supply Chain, that is intended "to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States" through the declaration of a national emergency. The EO would bar U.S. entities from buying or using the information and communications technology and services (ICT) from "foreign adversaries" if a determination is made that doing so would sabotage or subvert U.S. ICT, place U.S. critical infrastructure or its digital economy at "undue risk," or "poses an unacceptable risk" to national security or safety. The only "foreign adversary" that is positioned to threaten the U.S. in this fashion is China through Chinese companies such as Huawei, ZTE, and others that supply key goods to the supply chain of international technology firms and offers their own devices and services. It is likely that the EO is seen by the White House as a bargaining chip with China in negotiations on trade and tariffs and, as such, may never come fully into force as the Secretary of Commerce will receive discretion to modify the blanket ban on Chinese information and communications technology and services. Last year, the Department of Commerce replaced the seven-year ban on ZTE with $1 billion in sanctions at the behest of the President who tweeted his concern that the ban would result in too many lost jobs in China.

Further Reading

"Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products" – *The Wall Street Journal*
"The spy in your wallet: Credit cards have a privacy problem" – *The Washington Post*
"Israel eases rules on cyber weapons exports despite criticism" – *Reuters*
"How an NSA researcher plans to allow everyone to guard against firmware attacks" – *cyberscoop*
"Ransomware Attacks Are Testing Resolve of Cities Across America" – *The New York Times*
"How Amazon and Silicon Valley Seduced the Pentagon" – *ProPublica* and *Fortune*
"Federal officials raise concerns about White House plan to police alleged social media censorship" – *CNN*
"Start-ups are caught in middle of US-China tech cold war as investors pull back" – *South China Morning Post*
"T-Mobile 'Put My Life in Danger' Says Woman Stalked With Black Market Location Data" – *Motherboard*
"The quantum revolution is coming, and Chinese scientists are at the forefront" – *The Washington Post*
"The weaponisation of information is mutating at alarming speed" – *The Guardian*