MARKET INSIGHTS REPORT

FUTUREWEI TECHNOLOGIES

SE-1
March
2020

POLICY (PUBLIC AND REGULATORY)

Senate Hearing on 5G Supply Chain Security 2
Promoting U.S. International Leadership in 5G Act 2
FCC Order on 6GHz Still Likely at April Meeting 3
Delays in Regulatory Proceedings 3
White House 5G Security Report Lacks Substance 4
Secure 5G and Beyond Becomes Law 4
USG Investment in Nokia & Ericsson is a Bad Idea 5
USG Cybersecurity R&D Strategic Plan 6
DOT Releases Automated Vehicles 4.0 7
$9.7B Incentive to Clear C-Band 7
IBM Calls for Harmonized AI Regulations 8
U.S. Releases AI Guidelines 8
Congress Reviews Industries of the Future 9
Ongoing Challenges with 5.9GHz 9
Supply Chain Legislation 10
NIST Releases Privacy Framework V1.0 10
U.S. Announces New Policy on SEP and FRAND 11
FCC Proposal to Share 3.3-3.55GHz 11

POLICY (PUBLIC AND REGULATORY)

Senate Hearing on 5G Supply Chain Security

Up until Congress shifted its focus on combating the coronavirus in mid-March, there was little to no shortage of aggression towards or discussions surrounding China and Huawei inside the DC beltway. Exemplifying the attacks on Huawei, on March 4, 2020, the U.S. Senate Committee on Commerce, Science, and Transportation held a hearing to assess "*the security and integrity of the telecommunications supply chain*" and to explore "*the federal government's role in mitigating risks to telecommunications equipment and services in the U.S. and abroad*."

In identifying its list of experts on the topic, the U.S. Senate took the opportunity to make, yet another, political statement by excluding the leading global telecom suppler Huawei and instead limited its invite to Ericsson, Nokia and Intel along with the Competitive Carrier Association (CCA) and the Center for Strategic and International Studies (CSIS). To no one's surprise, the hearing quickly turned its focus to China and Huawei in particular, led by the representative from CSIS, James Lewis, who is a known antagonist.

During the hearing, Lewis argued that the best way to minimize risk to the 5G supply chain was to "eliminate" Huawei, claiming a partial ban as the United Kingdom has done poses some risk. CCA President's Steve Barry noted however that eliminating Huawei as a competitor will affect the cost of equipment made available by other vendors stating that in 6 months to 18 months, new technologies will drive down the costs of equipment for carriers.

To the extent the U.S. Government's (USG) aggression towards Huawei is dampened by recent events surrounding the coronavirus is yet to be seen. However, should this hearing serve as any type of indictor, it remains apparent some within the federal circles remain laser-focused on China.

Promoting U.S. International Leadership in 5G Act

In the U.S. Government's (USG) latest attempt to win the race to 5G and secure its leadership within the international standards community, two related pieces of legislation passed the House of Representatives (H.R.) in January 2020 and have made their way to the U.S. Senate for consideration.

H.R. 3763, *Promoting United States International Leadership in 5G Act of 2019*, and H.R.4500 - *Promoting United States Wireless Leadership Act of 2019*, while similarly call for greater U.S. involvement in standards setting organizations (SSO), approach the end-goal slightly differently. HR 3763 calls for the creation of an interagency group to brief Congress on (1) its strategy to promote U.S. leadership in the standards-setting bodies relevant to 5G technology; (2) its strategy for diplomatic engagement with allies and partners to share security-risk information related to 5G; (3) China's activities in standards-setting bodies for 5G technology, including the scope and scale of such activities; and (4) a strategy for engaging with private-sector stakeholders, academia, and federally funded research and development centers to propose and develop secure standards for 5G technology.

H.R. 4500, requires the Department of Commerce to assist trusted companies and relevant stakeholders with their participation in SSOs for telecommunications, wireless devices, and related equipment "*to enhance the representation of the United States and promote United States leadership in standards-setting bodies that set*

standards for 5G networks and for future generations of wireless communications networks." The SSO explicitly noted are ISO, IEEE, 3GPP and any SSO accredited by ANSI or ATIS; despite that fact that ATIS is not an accreditation group.

Given the similarities between the two bills, it is likely they will be consolidated at some point into a single bill and eventually signed into law. The greater question as to how the USG intents to "ensure" their standards leadership has yet to be answered.

FCC Order on 6GHz Still Likely at April Meeting

The U.S. regulatory decision regarding the reallocation and sharing of the 6 GHz band with Wi-Fi services appears to be still on track for the FCC Commissioners' meeting in April 2020, by which ending the 18-month global debate in the U.S., on what should happen in the 6 GHz band.

At stake, on one side of the debate, are existing incumbents in the band, like AT&T who have licensed spectrum for broadcast services, which have gone a record claiming the introduction of unlicensed wireless services in the band will case adverse interference to their services. On the other side, Wi-Fi advocates claim the 1200 mega-hertz of new spectrum (5925-7125 MHz) it seeks is critically important to maintain Wi-Fi's growth and its related social and economic values. And lastly, on the outside looking in, the licensed mobile carriers argue that they need at least some of the band for 5G services given the lack of mid-band spectrum for mobile services. For the most part, the FCC's position on 6 GHz has not changed throughout the debate and they seem determined to give the Wi-Fi community whatever it wants; both the 6GHz band and its adjacent ITS 5.9GHz band.

CTIA, the wireless industry's lobbying organization, remains committed however to pushing for some licensed use of part of the band. In several of their submissions to the FCC, CTIA agrees the U.S. needs more channels for the next generation of Wi-Fi, but 1200 MHz seems extreme. NCTA, not surprisingly, takes the opposite view and argues the entire 6 GHz band "*is the future home for Wi-Fi, both today and into the future*." For what its worth, Wi-Fi advocates believe they have already won the fight and are moving forward on developing and deploying Wi-Fi 6 for the 6 GHz band with work ongoing in IEEE 802.11 to develop the standards.

Delays in Regulatory Proceedings

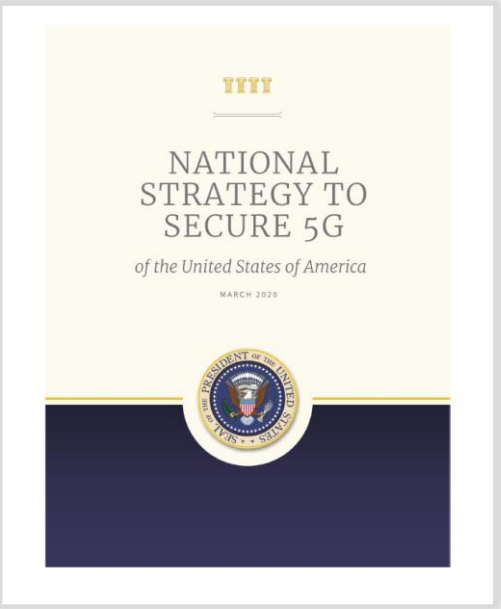
As the coronavirus continues to take its toll on the industry as a whole, regulatory agencies are trying their best to maintain some level and normalcy and advance important pending proceedings. In recent announcements, however, there have been setbacks. In recent public releases, the FCC has announced the delay of two spectrum auctions (Auction 105 and 106), has postponed their "Forum on 5G Virtualized Radio Access Networks", have extended the filing deadlines for numerous proceedings including net neutrality, and granted special licenses to most wireless carriers to extend/expand coverage during the outbreak. On the upside, many of the longer-term events and schedule remain intact, such as the C-Band auction which is still set for December 2020.

White House 5G Security Report Lacks Substance

Although lost in the noise of other news, the U.S. White House recently released its latest national strategy entitled "National Strategy to Secure 5G, March 2020" which intends to expand on how the U.S. will secure 5G infrastructures domestically and abroad. Based on reviews from multiple expert, however, many have commented that the report is "thin" on details, lacks substance, and offers nothing new to the debate.

As outlined in the report, the U.S. national strategy, as presented by the White House, is to "*lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide, arm-in-arm with our closest partners and allies*." To this end, in additional to other federal actions, the report highlights the FCC's plan to Facilitate America's Superiority in 5G Technology (the 5G FAST Plan) and repeats the U.S. commitment *"[to] participate in the development of international 5G security principles through frameworks, such as the Prague 5G Security Conference*."

Releasing the report now, despite the media noise, was meant to complement the "Secure and Trusted Communications Networks Act," which Trump also recently signed into law. That law, often referred to the "rip and replace" law, in part establishes (1) a mechanism to prevent communications equipment or services that pose a national security risk from entering U.S. networks, and (2) a program to remove any such equipment or services currently used in U.S. networks. More specifically, the bill prohibits the use of certain federal funds to obtain communications equipment or services from a company that poses a national security risk to U.S. communications networks (e.g., Huawei). And lastly, the FCC must publish and maintain a list of such equipment or services.



While indeed thin on specifics, the report does touch on various network-related aspects of interest including: (1) *Managing the Supply Chain Risks in United States Government Infrastructure - Including 5G*; (2) *Addressing the Risk of 'High-Risk' Vendors in United States 5G Infrastructure*; (3) *Developing and Promoting Implementation of International 5G Security Principles*; and (4) *Promoting United States Leadership in International Standards Development and Adoption*.

Secure 5G and Beyond Becomes Law

Originally introduced in the U.S. Senate, S.893, Secure 5G and Beyond Act of 2020 became law in late March 2020, less then one year after its introduction gaining strong bipartisan support.

In the law, Congress calls on the Administrative to "*develop a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure in the United States and to assist allies and strategic partners in maximizing the security of next generation mobile telecommunications systems, infrastructure, and software, and for other purposes*." To this end, Congress proposes a two-prong approach.

First, an inter-governmental group comprised of key agencies will be formed including the FCC, Dept. of Commerce, Homeland Security, National Intelligence, Attorney General, the Dept. of State, the Dept. of Energy, and the Dept. of Defense to assist the White House in developing a strategy addressing the provisions of the law related to the security of next generation network. The strategy is to be called the "National Strategy

to Secure 5G and Next Generation Wireless Communications." In addition, the group will: (1) assess options to protect the competitiveness of U.S. companies; (2) to assist U.S. allies with technical expertise to maximize security; (3) to develop plans to promote "responsible global development and deployment" of 5G and next generations wireless networks; and (4) in the promotion of "responsible development," consider efforts to enable robust international engagement and leadership in the development of international standards.

Second, in parallel to the abovementioned network security, the law instructs the White House to develop and submit to Congress an implementation plan for strategies to address a whole host of related items. Several issues named in the law include: (1) a detailed assessment of potential threats and vulnerabilities posed by 5G networks and methods to address these vulnerabilities; (2) the identification and assessment of the global competitiveness and vulnerabilities of U.S. manufacturers and suppliers of (5G and beyond wireless) communications equipment; (3) the development of a plan for engaging with communications equipment providers (and other) to encourage maximizing their participation in standards setting organizations; and (4) a plan for research and development by the Federal Government, in partnership with trusted suppliers and allies, to reach and maintain U.S. leadership in 5G and beyond (wireless) systems.

The recommendations and findings stemming from both of these efforts ("the reports") are due back to Congress around the September 2020 timeframe for further consideration. At that time, we will either learn how the USG proposes to implement these actions or we'll see a request for additional time. Only time will tell at this point. The 180-days given by Congress to complete these actions is considered aggressive.

USG Investment in Nokia & Ericsson is a Bad Idea

Over the last several months, numerous reports have surfaced with respect to the U.S. Government's ("USG") possible investment in communication equipment vendors NOKIA and Ericsson as a means to combat Huawei and its global presence.

Since May 2019, when the USG placed Huawei on its "Entity List" for export control, it has aggressively pursued every legal means to remove existing Huawei equipment from its communication networks while also banning future deployments. It also has been actively lobbying its allies to follow suit on the grounds of the overarching and overused term of national security. The US' latest volley of attempts comes from government statements that the USG could directly invest in or purchase Huawei's competitors as a means to bolster their capabilities in effort to offer U.S. carriers' an alternative.

As a case to point, the US Attorney General William Barr, has gone on public record affirming the USG's efforts to invest in Huawei's competitors by saying that the USG and/or a leading US tech firm should buy all or part of one of Ericsson or Nokia in order to fill the vacuum in the availability of trusted vendors in the global communications market. Also, in a related report, the US Secretary of Defense Mark Esper told attendees at the Munich Security Conference that "America was working with vendors like Ericsson, Nokia, Samsung and beyond to develop alternative 5G technologies." Specifics were not provided. But, obviously, not everyone agrees with the USG positions.

LightReading recently reported that AT&T's CEO Stephenson and others have said that USG's investment in Huawei's rivals was a bad idea noting that governments have had a bad track-record investing in public and private companies. Instead, Stephenson and others, believe there's a better way for the US to tackle the situation and is supporting an alternative approach to Huawei. An approach which, if successful, in all likelihood will also cause a bifurcated industry between CHINA and the USA.

Recently, White House Economic Adviser Larry Kudlow issued a plan calling for the USG to invest into developing software for 5G (not in purchasing rival companies) by US-based companies and have claimed AT&T, Dell, Microsoft and others support the proposal. As reported, *"[t]he plan would build on efforts by some US telecom and technology companies to agree on common engineering standards that would allow 5G software developers to run code atop*

machines that come from nearly any hardware manufacturer. That would reduce, if not eliminate, reliance on Huawei equipment," said by Larry Kudlow. Kudlow also commented that ***"[t]he big-picture concept is to have all of the US 5G architecture and infrastructure done by American firms, principally***." News of the plan was initially reported by the Wall Street Journal. A subscription is required to access the full article.

To help drive the effort, a group of US Senators led by Senator Mark Warner, is proposing the US provide more than $1 billion "*to invest in Western-based alternatives to Chinese equipment providers Huawei and ZTE*." Under his proposal, the Federal Communications Commission would funnel at least $750 million into O-RAN technologies and the US would set up a $500 million Multilateral Telecommunications Security Fund to speed up "*the adoption of trusted and secure equipment globally*." Funds would be available to "foreign partners". Warner is also calling for the increase in US leadership in international standards organizations by encouraging greater US participation. Increasing US involvement in SSOs has been a common theme since this all begun.

FCC Chairman Pai has also announced that the agency will hold a Forum on 5G Virtualized Radio Access Networks on March 26, 2020. The purpose of the forum is to convene experts "at the forefront of the development and deployment of interoperable, standards-based, virtualized radio access networks… to discuss this paradigm-shifting approach to 5G network deployment." Chairman Pai is quoted in the release announcing the forum saying that one way to advance the priority of promoting U.S. leadership in 5G "*is through the development and deployment of more secure, cost-effective 5G network components. Virtualized radio access networks could help us do that*." Details on the agenda and speakers will be announced at a later date.

Based on USG actions over the past year and its relentless attacks on Huawei, intentions appear clear. Yet, recent tweets from the U.S. President have also suggested that people may be overreacting saying that people are getting carried away with using "*a fake term of national security*." The saga will likely continue as these various efforts progress.

USG Cybersecurity R&D Strategic Plan

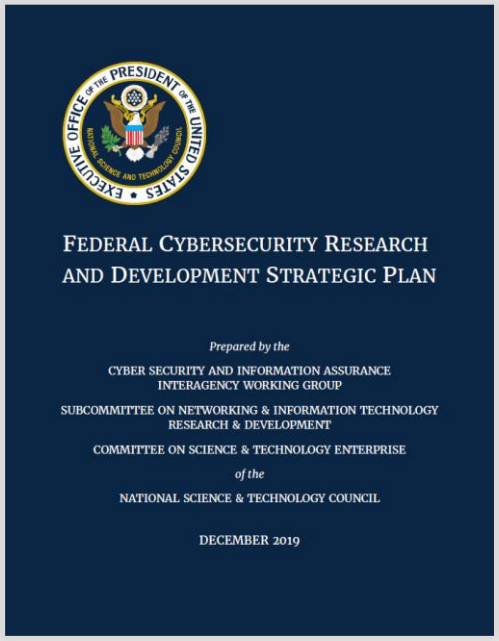
In December 2019, the U.S. National Science and Technology Council ("NSTC") released its "Federal Cybersecurity Research and Development Strategic Plan" providing a guide to the overall direction of federally funded R&D work in cybersecurity.

As outlined in the plan, there are six (6) priority areas for R&D funding. Provided are the six areas and a brief description of their goals:

Artificial Intelligence: Goal - Simulate different decision-support scenarios with respect to threat models, including attacker/defender strategies related to specific AI/ML implementations; Expand and explore new AI-based techniques for cybersecurity tasks beyond malware and intrusion detection; Develop models, definitions, and metrics of security and trust that can be used to evaluate AI cybersecurity systems and AI-based cybersecurity controls

Quantum Information Services: Goal – Design "type-safe" quantum programming languages; explore new theoretical and experimental methods to probe quantum states, quantum processes, and their quantum properties; draft standards for quantum-resistant cryptography; understand how quantum technologies can be exploited for attacks on classical and/or quantum systems and understand security threats against quantum devices and their supply chain

Trustworthy Distributed Digital Infrastructure: Goal - Develop standards to support seamless, end-to-end security across interconnected networks, trust domains, topologies, networking paradigms, and mobile devices and mobile network layers; develop end-to-end security and key management capabilities offering secure, highly resourced nodes to interoperate with resource-limited edge and IoT devices; develop technologies to sustain autonomous management of security across the communication infrastructure



Privacy: Goal -- Develop research methods that can reliably and validly sample, measure, and represent people's privacy desires, expectations, attitudes, beliefs, and interests; develop methods and technologies that can identify privacy violations and privacy harms; devise frameworks that integrate safety, security, and privacy requirements; foster techniques and models that can systematically assess and quantify privacy risks; develop models, techniques, and evaluation metrics for redress and recovery from privacy violations

Secure Hardware & Software: Goal -- Develop novel processes, techniques, and mechanisms that protect against reverse-engineering efforts; develop mechanisms and tools that verify the security properties of hardware; develop secure debug and testing techniques; develop new software development methodologies that allow rapid revision and regression against security goals; develop secure update mechanisms that support the full range of product formats; develop cost- and threat-proportionate integrated root-of-trust alternatives for various hardware devices, ranging from low-cost IoT devices and networked sensor devices to server computers

Education & Workforce Development: Goal -- Accelerate adoption of a modern taxonomy of the cybersecurity workforce; conduct research on effective models to educate individuals of different backgrounds and ages; research innovative ways to develop talent in all sectors of society to build the cybersecurity workforce; support experiential learning, such as apprenticeships, internships, job-shadows, and other employer-educator partnerships; and focus not only on developing expertise but also on research on how the education and training ecosystem can develop interdisciplinary approaches that support innovation

DOT Releases Automated Vehicles 4.0

On January 8, 2020, the U.S. Department of Transportation ("DOT") and National Science & Technology Council ("NSTC") released the fourth version of its Automated Vehicles series "*Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0* (AV 4.0)."

Building upon the previous three versions, AV4.0 outlines the USG's policy approach to AV technologies. In it, the USG details its authority to regulate, lists its research programs, and summarizes its investments strategy across the various USG agencies. In an effort to ensure that it maintains the lead in AV research, development, and integration, the report also highlights USG's efforts to be proactive by providing guidance, best practices, proposed research and pilot programs to help stakeholders in their investments. And lastly, it details the USG's 10 principles to foster research, development including safety, privacy, mobility, innovation, and standardizations.

A snapshot of current State and federal efforts around AV policies, including more details on AV4.0, is provided as an Appendix to this report. Comments to AV4.0 are due in April 2020.

$9.7B Incentive to Clear C-Band

At the latest FCC Open Commission Meeting on February 28th, the FCC Commissions approved two critical proceedings related to the clearing of the C-Band and its associated auction.

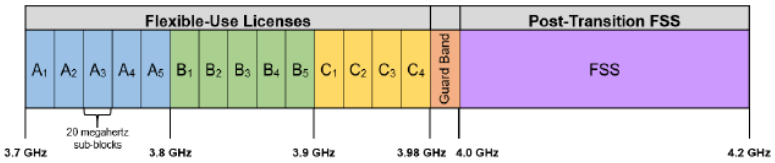
In the FCC Public Notice, Auction of Flexible-Use Service Licenses in the 3.7–3.98 GHZ Band for Next-Generation Wireless Services, the FCC released details associated with the clearing of the C-Band and seeks comment on the procedures to be used for auctioning the licenses in the band (Auction 107); which is to commence on December 8, 2020.

To clear the band and make it ready for (flexible) commercial use, FCC Chairman Ajit Pai is proposing a $9.7 billion incentive to the C-Band satellite incumbents to vacate the band. According to the C-band Draft Order, Expanding Flexible Use of the 3.7 to 4.2 GHz Band, Intelsat would be eligible for up to $4.85 billion if relocated by the 2021 and 2023 clearing deadlines. SES would be eligible for $4 billion, Eutelsat for $467 million, Telesat for $374 million and Star One for $13.6 million.

The Order would also (1) transition 280 megahertz, plus a 20-megahertz guard band, from incumbent use to flexible-use by September 30, 2025 through a Commission-led public auction; (2) Require incumbent FS licensees to relocate their point-to-point links to other bands, by September 30, 2023; and (3) provide both incumbent FSS and FS licensees with reimbursement of reasonable relocation costs paid by flexible-use licensees as a condition on their license.

Post-transition of incumbents, the FCC is proposing to create two categories of generic blocks in each Partial Economic Area (PEA); namely, Category A which would consist of blocks in the lower 100 megahertz (3.7–3.8 GHz), and Category BC which would consist of blocks in the remaining 180 megahertz (3.8–3.98 GHz).

Figure 1: Post-Transition 3.7–4.2 GHz Band Allocations in the Contiguous United States



The FCC plan appears to have a lot of industry support and is expected to be approved.

IBM Calls for Harmonized AI Regulations

In January 2020, IBM announced the launched of its newest initiative, called "Policy Lab," to help advise and guide policymakers on critical public policy issues. The Lab's aim is to develop and advocate for policies towards enabling new technologies while meeting present and future demands. One of the Lab's high priorities is to create rules that eliminate bias in AI systems and plan to work in concert with standards-setting bodies and governments to this end.

In a paper released by the Lab, "Precision Regulation for Artificial Intelligence**",** IBM notes that "62% of Americans and 70% Europeans prefer a precision regulation approach for technology, with less than 10% in either region supporting broad regulation of tech. 85% of Europeans and 81% of Americans support consumer data protection in some form, and 70% of Europeans and 60% of Americans support AI regulation." The paper also proposes five (5) policy imperatives for companies to follow including the need to designate a lead AI ethics official and to be transparent in how they use AI.

Other policy directions released by the Lab include "Precision Regulation and Facial Recognition," "IBM and Climate Change: Early Action, Sustained Results, and Support for a Price on Carbon.", and "A Precision Regulation Approach to Stopping Illegal Activities Online."

U.S. Releases AI Guidelines

Last February 2019, Executive Order 13859, "*Maintaining American Leadership in Artificial Intelligence*" was released in effort to spur U.S. investment in Artificial Intelligence (AI). Since then, federal agencies have been working towards the objectives and goals outlined within the Order to include the release of guidelines to advise on regulatory requirements. As outlined in the Order, the Office of Management and Budget (OMB), in coordination with the Office of Science and Technology Policy (OSTP), the Domestic Policy Council (DPC), and the National Economic Council (NEC), was charged with providing guidance to federal agencies regarding the review and release of regulatory and nonregulatory requirements that aim to reduce barriers to the development and adoption of AI technologies.

In the released draft Memorandum, *Guidance for Regulation of Artificial Intelligence Applications,* OMB and team have outlined 10 guiding principles for agencies to consider when setting policies and/or regulations around AI. As typical of

the U.S. efforts to promote market-based regulations, in sum, the guidance emphasized the need for a light-touch regulatory approach. More precisely, as noted in the guidelines "…*federal agencies must avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth. Where permitted by law, when deciding whether and how to regulate in an area that may affect AI applications, agencies should assess the effect of the potential regulation on AI innovation and growth. Agencies must avoid a precautionary approach that holds AI systems to such an impossibly high standard that society cannot enjoy their benefits*."

Michael Kratsios, the United States CTO, also recently blogged about the release in which he stated that the new principles intend to promote the development of trustworthy AI and encourages regulators to consider **fairness, transparency, safety, and security** in their proceedings. "Agencies should also pursue verifiable, objective evidence for their policy decisions, basing technical and policy decisions on the best possible scientific evidence", he continued.

Congress Reviews Industries of the Future

The Senate Committee on Commerce, Science, and Transportation recently convened a hearing, "*Industries of the Future*," to examine how the U.S. can maintain its global economic edge in key technologies; namely, AI, advanced manufacturing, quantum computing, biotechnology, and 5G. Witnesses included leadership from NIST, National Science Foundation (NSF), OSTP, and FCC.

In responding to Congress' questions regarding U.S. approach to and its preparedness in responding to these technologies, common themes from the witnesses included (1) the need for federal government to remove barriers, streamline processes, and avoid imposing burdensome or preemptive regulation; (2) the importance for U.S. to win the race to 5G and thereby the need for more spectrum; (3) the need for funding of research and development for quantum computing; and (4) the need for federal agency engagement in standards development.

The information presented during the hearing will assist the committee membership in finalizing exiting proceedings and setting future legislations.

Ongoing Challenges with 5.9GHz

What ultimately happens in the current FCC 5.9 GHz proceeding remains to be seen with varying opinions readily available on the asking. But in response to the FCC released, but yet published (to-date), "*Use of the 5.850-5.925 GHz Band*," Notice of Proposed Rulemaking (NPRM), the Department of Transportation (DOT), has provided insights in to its preliminary technical assessment of the proceeding and has outlined its concerns with the Commission's proposal.

As stated in DOT's assessment, their primary concern, as expected, is with the reallocation of 45-megahertz from its assigned 75-megahertz for ITS and, as such, its impact on delivering safety of life services. According to DOT, the proposed FCC actions would delay deployments of life-saving services, not accelerate which the FCC promotes, by 5 years in order "*to develop, standardize, and deploy equipment – either existing concepts in different spectrum or new concepts in existing spectrum*." Out-of-band-emission (OOBE) levels are also likely to create interference in the remaining 30-megahertz of ITS spectrum raising questions about the reliability of the services; either C-V2X or DSRC. OOBE limits are currently undefined in the current NPRM.

Similar concerns on the reassignment of the spectrum were also expressed by the House Committee on Transportation and Infrastructure who has jurisdiction over commercial transportation. In a letter sent to the FCC Chairman and Commissioners, the committee expressed its alarm over the FCC's proposal to reallocate the band to unlicensed operations noting its potential "*to prevent many of the 37,000 traffic fatalities each year by impeding the development and deployment of safety-critical technologies*."

Despite the concerns expressed by the other government authorities (DOT and the House Committee), FCC Chairman Pai appears unphased and has doubled down on he's proposal to reallocate the band.

Supply Chain Legislation

Despite expressed concerned from some U.S. telecom executives that they are likely to get "boxed in" with the U.S. Government's (USG) actions to ban Chinese equipment deemed of threat to national security, representatives in the U.S. Congress is expected to restart talks shortly after the current impeachment trial to advance legislation on banning the future use of such equipment and are proposing funds to help operators remove existing equipment ("rip and replace") from the U.S. networks.

Of particular interest, several pieces of legislations are currently in-play regarding 5G-related technologies and securing the national communication network. Legislation of interest include the House-passed Secure and Trusted Communications Networks Act (HR-4998), its companion legislation Senate Commerce-cleared U.S. 5G Leadership Act (S-1625), the Secure 5G and Beyond Act (HR-2881), the Promoting U.S. International Leadership in 5G Act (HR-3763), and the Promoting U.S. Wireless Leadership Act (HR-4500).

HR-3763, of particular interest, illustrates USG's desire to engage in international standards setting organizations, such as ITU, to ensure U.S. leadership in 5G and beyond. Further the bill states that *"[t]he State Department shall report to Congress on (1) its strategy to promote U.S. leadership in the standards-setting bodies relevant to 5G technology; (2) its strategy for diplomatic engagement with allies and partners to share security-risk information related to 5G; and (3) China's activities in standards-setting bodies for 5G technology, including the scope and scale of such activities*."

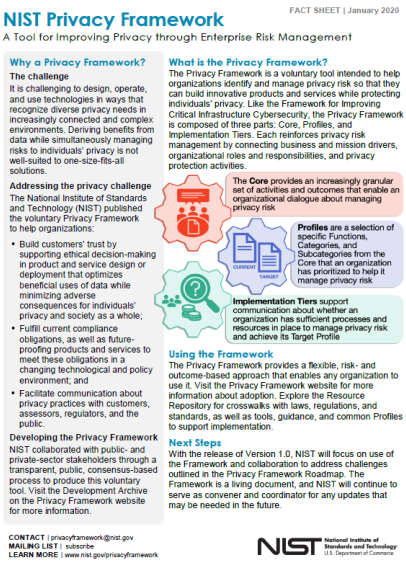
The USG has long been under the impression that China has the ability to dominate the standards setting organizations and their processes to its sole advantage. HR-4500 direct NTIA to encourage U.S. companies and others to participate in international standards-setting bodies to the benefit of U.S. -- that is, in ways in which the U.S. has condemned China for its supposed involvement in standards.

NIST Releases Privacy Framework V1.0

In January 2020, after nearly 18-months of development, NIST has released Version 1.0 of the NIST Privacy Framework: *A Tool for Improving Privacy through Enterprise Risk Management*.

The Privacy Framework closely follows the structure of the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), which it published several years ago. Like the Cybersecurity Framework, the Privacy Framework is composed of three parts: Core, Profiles, and Implementation Tiers.

As expressed by NIST, the Privacy Framework was developed to support organizations in (1) building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data; (2) fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and (3) facilitating communication about privacy practices with individuals, business partners, assessors, and regulators.



Over the next year, NIST intends to engage with stakeholders to promote the use of the Framework including industry conferences and other outreach activities such as webinars and workshops. Their first webinar was held on January 29, 2020 which can be seen here.

U.S. Announces New Policy on SEP and FRAND

The Department of Justice (DOJ), United States Patent and Trademark Office (USPTO), and National Institute of Standards and Technology (NIST), recently issued a joint statement on remedies for Standard-Essential Patents ("SEP") and fair, reasonable, and non-discriminatory ("FRAND") terms. As noted in the press release:

"The Statement clarifies that a patent owner's promise to license a patent on F/RAND terms is not a bar to obtaining any particular remedy, including injunctive relief. The agencies make clear that no "special set of legal rules" apply to SEPs, and the courts, the U.S. International Trade Commission, and other decision makers are able to assess appropriate remedies based on current law and relevant facts. According to the Statement, "The particular F/RAND commitment made by a patent owner, the [standard development organization's] intellectual property policies, and the individual circumstances of licensing negotiations between patent owners and implementers all may be relevant in determining remedies for infringing a standards-essential patent, depending on the circumstances of each case."

FCC Proposal to Share 3.3-3.55GHz

The FCC has finally submitted its Notice of Proposed Rulemaking (NPRM), *Facilitating Shared Use in the 3.1-3.55 GHz Band*, for publication to the Federal Register whereby starting the clock for public comments. Comments are due Feb. 21 with replies March 23.

The NPRM proposes to clear the 3.3-3.55 GHz band by removing non-federal secondary radiolocation and amateur allocations and seeks comments on how best to relocate the incumbent users to either the 3.1-3.3 GHz band or other frequencies.

In the NTIA study of the band, they have identified the 3.45-3.55 GHz band as the most promising portion for sharing in the near term and is continuing to perform feasibility studies in collaboration with the Department of Defense (DOD) on sharing the band as well as the entire 3.1-3.55 GHz band with existing and future federal users. The adjacent band, 3.55-3.7GHz, is the Citizen Band Radio Service (CBRS) band where services are shared utilizing a three-tier priority access approach. Comments from CBRS advocates (i.e., GOOGLE, Federated Wireless, Cisco, and Ruckus) in support of extending the CBRS band to include this band is expected.