DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

The National Strategy to Secure 5G Implementation Plan

Request for Public Comments

Docket No. 200521-0144

COMMENTS OF AT&T SERVICES, INC.

AT&T Services, Inc., on behalf of itself and its affiliates (together, "AT&T"), respectfully submits these comments in response to the *Request for Public Comments* in the above-referenced proceeding. In that *Request*, the Department of Commerce's ("Department") National Telecommunications and Information Administration ("NTIA") seeks comment "to inform the development of an Implementation Plan for the National Strategy to Secure 5G."[1] The *Request* stems from the Secure 5G and Beyond Act of 2020, which the President signed into law on March 23, 2020, and which requires development of a strategy to ensure the security of next generation wireless communications systems and infrastructure.[2] The *Request* details the Administration's National Strategy to Secure 5G (Strategy), published on the date of enactment to fulfill the requirement in the Act. The strategy is focused on four lines of effort, which our comments address in the following order: 1) Line of Effort One: Facilitate Domestic 5G Rollout; (2) Line of Effort Three: Address Risks to U.S. Economic and National Security During Development and Deployment of 5G Infrastructure Worldwide; 3) Line of Effort Four: Promote Responsible Global Development and Deployment of 5G; and 4) Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure.

[1] *The National Strategy to Secure 5G Implementation Plan*, Request for Public Comments, 85 Fed. Reg. 32016 (May 28, 2020).

[2] *Id.* At 32017.

Introduction:

At the outset, it is important to note the effectiveness of U.S. wireless networks in handling the significant increases in network demands during the COVID-19 pandemic. This robust network resiliency is a direct result of the competitive nature of the wireless industry, with carriers vying for customers by investing in and building out their networks to provide reliable and cutting-edge services that consumers demand. The investment and buildout supporting our networks is also a result of the U.S. Government's "light touch" approach to regulation, which has allowed carriers to freely operate their businesses without a heavy regulatory hand, while still addressing key regulatory reforms that are needed to expedite deployment of 5G. We commend, for example, the FCC's comprehensive strategy to Facilitate America's Superiority in 5G Technology (the 5G FAST Plan). The strategy is intended to facilitate the availability of more spectrum, update infrastructure policy, and modernize outdated regulations. Forward thinking regulatory approaches like these have helped companies like AT&T more quickly deploy new generations of technology.

Continuing to promote a regulatory environment that spurs the development and deployment of 5G is critical. 5G is the latest and arguably most significant new generation of mobile communications. The first generation brought voice-only mobile services in the 1980s; 2G enabled texting; 3G allowed the first mobile internet access; and 4G enabled mobile broadband, which unleashed a revolution in the mobile ecosystem, including entertainment and business models based on video streaming and mobile applications. 5G promises even greater leaps in the applications and business models that it will support.

While the U.S. Government can spur the development and deployment of 5G, we also believe that it is important that NTIA focus future government efforts on issues that need further development, as opposed to boiling the ocean around 5G. For example, there have been a wide variety of "security" issues raised about 5G. These can range from the security of the 5G network architecture itself, the integrity of the 5G standards process, the 5G (and greater) supply chain and the pace of 5G deployment. As we outline in our comments, there is ongoing work in both standards bodies and within the U.S. government to address many of these issues, in particular 5G network security and standards, and NTIA should therefore focus its efforts in areas where further government engagement is potentially necessary and will be most beneficial.

These areas include fostering supply chain network diversity and expediting 5G deployment, including making available more mid-band spectrum.

I. Line of Effort One: Facilitate Domestic 5G Rollout.

This line of effort concerns the steps the U.S. Government can take to facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem. These efforts should focus on facilitating spectrum availability, streamlining local permitting, and fostering and promoting the research and testing on and development of new technologies and architectures, that will help maintain U.S. leadership in 5G and create an environment that encourages private sector investment in 5G technologies and beyond.

Regulatory approach and facilitating spectrum availability

Regarding spectrum policy, government should continue efforts to free up radiofrequency spectrum for 5G, and in particular spectrum (between 3 GHz and 8 GHz), particularly in the 3.1-3.55 GHz range. Mid-band spectrum is particularly important for 5G because it offers a balance between wide geographic coverage and greater capacity and speed. By contrast, the high-band millimeter-wave spectrum, which has already been made available, has lower propagation characteristics and allows for large volumes of data to be transmitted over relatively short distances. Many countries are currently relying exclusively or predominantly on mid-band spectrum for 5G deployment. As a result, a significant amount of investment and innovation in 5G is expected to center around the use of mid-band spectrum, making it important for the U.S. both to contribute to and benefit from this innovation.

As part of its 5G FAST Plan, the FCC has already begun a series of auctions to make available spectrum necessary for 5G deployment. The FCC plans to proceed with an auction of the licensed portion of the Citizens Broadband Radio Services (CBRS) band in July 2020. In addition, the Commission recently announced a plan to free up C-band spectrum currently being used by satellite providers. As noted above, additional mid-band spectrum should be cleared and auctioned for 5G as soon as possible to ensure that entities that wish to invest in 5G deployment have the critical spectrum resources to do so. NTIA is required through the Mobile Now Act to review the possibility of sharing the 3.1-3.55 GHz band and has already stated that the 3.45-3.55 GHz band is a good candidate band for sharing. NTIA should move forward with making this band available for auction and should also see if additional spectrum below 3.45 GHz could be

made available at the same time, such as 3.3-3.55 GHz (a larger block of spectrum provides for greater bandwidth and hence capacity and more competitors).

Streamlining Local Permitting

Second, government should also continue steps to streamline or eliminate local permitting and other barriers to deployment of 5G infrastructure. 5G will entail a greater and denser number of small cell sites than previous generations of wireless technology, although macro cell sites will continue to be important to provide coverage. Although we recognize that local governments have a legitimate interest in decisions on the location of these small call placements, it is important to ensure that local authorities do not demand unreasonable concessions from wireless carriers, or go even further to ban small cell placement in certain areas or jurisdictions. In the same vein, we are supportive of actions the FCC has taken to implement rules to eliminate delays in issuing and unjustified denial of local infrastructure permits. We also support legislative action, such as the Streamline Small Cell Deployment Act (S. 1699). Continuing efforts to reduce barriers to local deployment are critical to encouraging private sector investment in 5G infrastructure.

Fostering and incentivizing research, development, testing, and evaluation of new technologies and architectures

The White House Office of Science and Technology has rightly characterized research and development as "vital" to maintaining the U.S.'s leadership role and ensuring the timely and strategic adoption of 5G.[3] The National Institute of Standards and Technology has also urged prioritization of research that will support the transition to more dynamic, agile, and innovative wireless networks.[4] We urge government to take steps to foster research, development, testing and evaluation of new technologies and 5G initiatives, and to support collaborative industry ventures.

Passing the Utilizing Strategic Allied Telecommunications Act (S. 3189 and H.R. 6624) or similar legislation, would be an important step in the right direction. These measures focus

[3] Executive Office of the President of the United States, *Research and Development Priorities for American Leadership in Wireless Communications*, Office of Science and Technology, at ii (May 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/Research-and-Development-Priorities-for-American-Leadership-in-Wireless-Communications-Report-May-2019.pdf.

[4] U.S. Department of Commerce, National Institute of Standards and Technology, *Future Generation Wireless Research and Development Gaps Report*, at 5 (Feb. 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1219.pdf.

on promoting adoption of interoperable equipment—equipment that can work or interoperate with equipment from other vendors. Interoperability is important as it allows for operators to build networks using various vendors choosing equipment based on performance, pricing, and security; and it avoids requiring operators to lock-in with one equipment vendor.

The Senate bill would devote at least $1.25 billion towards funding research into technologies that will increase competitiveness in the 5G supply chain and encouraging the adoption of "secure and trusted" 5G technologies worldwide.[5] Both bills would fund a $750 million Public Wireless Supply Chain R&D Fund, which would be used for grants of up to $20 million for research and commercial applications of technologies that would support competitiveness and interoperability in the 5G supply chain. The Senate bill would grant an additional $500 million to create a Multilateral Telecommunications Security Fund to develop and implement secure telecommunications technologies in conjunction with foreign partners. Key aspects of the legislation have reportedly also been included in the FY 2021 Intelligence Authorization Act, which the Senate Select Committee on Intelligence recently passed out of committee. We urge Congress to pass this legislation into law and provide financial support for these technology developments, including Open RAN, which in turn may shape policies currently under consideration in other parts of the world.

We also encourage government to support private research and development initiatives through grants and tax incentives, as well as the work of academic research centers in the United States. Universities often excel at research that can be difficult to monetize. Government has long provided vital assistance to these research efforts, such as National Science Foundation's support for the NYU Wireless Center, which advances technologies in mmWave channel modeling, 5G channel model simulation, and the distributed core architecture, and for the Wireless Networking and Communications Group at the University of Texas at Austin, which conducts important research into increasing wireless network capacity.

Additionally, government should foster industry collaboration to support the advancement of 5G. For example, government could encourage and support collaboration through a research consortium or partnerships among network equipment suppliers. Financial

[5] Jon Brodkin, *US May Subsidize Huawei Alternatives with Proposed $1.25 Billion Fund*, ARS Technica (Jan. 15, 2020), https://arstechnica.com/tech-policy/2020/01/us-may-subsidize-huawei-alternatives-with-proposed-1-25-billion-fund/.

support such as through direct subsidies and tax incentives (i.e. such as by offering research and development tax credits to participating vendors, or tax credits to operators for purchasing products that emerge from these efforts) is an essential catalyst for such collaboration. Government could also make available its research laboratories, and potentially other relevant resources, and provide a coordinating function to bring together representatives from government, industry, and academia, which would help ensure that relevant stakeholders are working collaboratively toward a common and mutually beneficial outcome.

II. Line of Effort Three: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide.

This Line of Effort focuses on the potential opportunities created by 5G around the world, on economic and national security risks, on promoting vendor diversity, and on fostering market competition.

Worldwide opportunities created by 5G

As mentioned above, 5G is the latest and arguably most significant new generation of mobile communications. 5G will change the way we work, play, and live, paving the way for the fourth industrial revolution. New 5G-supported technologies include everything from connected cars and cities to augmented and virtual reality. Ultra-high definition video will move towards public adoption, all thanks to the huge leaps in capacity and speed that 5G will offer.

First, by making today's wireless networks faster, more reliable, and more secure, 5G will allow improvements to the myriad of mobile broadband applications that smartphones have enabled, and that consume an ever-increasing amount of data and bandwidth. Early 5G deployments are already ten times faster than today's 4G networks, and, when fully realized, 5G mmWave offers to deliver speeds up to 100 times faster.

Second, 5G will not just improve today's popular mobile broadband applications but will also enable a boundless range of new use cases. 5G networks along with moving the applications to the edge will dramatically reduce latency — the amount of time it takes for a signal to travel across the network — by a factor of five or more. This will open up wireless communications to new applications that require near-instantaneous data transfers, such as industrial automation, virtual reality entertainment, connected vehicles, telesurgery, and many others.

Third, 5G will also expand the number of possible connections in a given space — from about 4,000 devices per square kilometer under 4G, to about a million. This will enable the massive Internet of Things (IoT) — the proliferation of devices that maintain constant connections with the "cloud," including everything from personal health sensors, to connected cars and appliances, and much more.

These advances are expected to bring about massive economic growth. Analysts predict 5G technologies will generate $13.2 trillion in sales activity across multiple industries by 2035 — approximately the equivalent of current U.S. consumer spending. 5G is expected to support, by some counts, 22 million jobs by 2035 – three times as many workers as are currently employed by the top ten companies on the 2019 Fortune 1000.

History demonstrates that the countries or regions that lead wireless transitions reap huge rewards. The United States led the world in deploying 4G LTE. This enabled the U.S. to enjoy massive economic benefits — $445 billion in U.S. GDP in 2016 alone, by some estimates.

5G Supply Chain and Open RAN

As discussed in the National Security Telecommunications Advisory Committee (NSTAC) *Letter to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*, there are concerns about the growing consolidation of manufacturers, and the long-term implications for 5G and the broader communications and Internet technology supply chain. This concern is particularly acute in the Radio Access Network (RAN) portion of the network where there are a limited number of RAN equipment suppliers.

A primary root of this concern is the growing presence of reportedly subsidized competition from China. In particular, Huawei has grown rapidly and achieved significant scale as the preferred supplier to the vast Chinese market. Compounding its size advantage, Huawei reportedly receives financial support from the Chinese government, which could allow it to undercut rivals on price. Huawei has also been able to increase its research and development spending considerably as part of its attempt to grow market share. Huawei's growth and position poses a special challenge because its growth has further concentrated the marketplace, but it also fails to offer a reasonable competitive alternative to U.S. carriers due to U.S. Government restrictions. The consolidation of vendors has decreased vendor diversity and created challenges for new entrants. Upfront costs related to labor, equipment, and research and development all

work to discourage new communications vendors from competing with established players. However, there are opportunities to correct this in the future.

As networks have evolved toward open architectures, Software Defined Networking (SDN) and Network Function Virtualization (NFV) may provide an option to address supply chain concerns by driving the industry toward a more interoperable, modular network design that will foster competition between suppliers and lower barriers to entry for new entrants in the marketplace. To support these developments, in 2018, AT&T and other companies launched the O-RAN Alliance which was formed to help operators clearly define requirements and help build a supply chain to realize these objections. Other organizations such as the Telecom Infrastructure Project (TIP), which has a liaison relationship with O-RAN, are working on similar objectives.

It is critical that the U.S. put in place the right policy framework to allow the technical solutions championed by these groups to succeed. In the short-term, government can support more innovation in the ecosystem by promoting policies that support interoperability, vendor diversity and competition in the supply chain. In particular, we urge NTIA to review the recommendations contained in the NSTAC's Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem issued September 3, 2019.

Economic and National Security and 5G

There has been ample public discussion surrounding 5G – the security of the network itself, that China is having undue influence in standards, and that the use of Chinese equipment could compromise networks. As discussed above, it is important to distinguish between network security, which provides enhancements in 5G over 4G, and supply chain security, which continues to create concerns around the world as countries choose vendors for their 5G build-outs. While government has dedicated a significant effort to assessing the risks around certain Chinese equipment suppliers, we believe greater focus needs to be directed at the longer term national and economic security risk stemming from vendor concentration in the supply chain, in particular in the RAN. Consistent government commitment to ensuring a diverse, competitive supply chain long-term is critical to economic and national security.

Specifically, government should ensure that 5G deployments for government use, such as those of the Department of Defense, use equipment from trusted and preferred suppliers. This is consistent with long-established preferences for a competitive environment for government

contracts and will help bolster long-term economic and national security. This approach can help sustain a market for competitive supply while falling well short of the highly regulatory model that other countries have employed involving direct investment in or state ownership of an equipment supplier.

Government can also financially support private investments, such as the $9 billion the FCC recently announced it would award to carriers deploying 5G in rural areas. Any such investment should likewise preserve existing diversity among network equipment vendors. For example, the FCC's recent step of requiring Universal Service Fund dollars to be spent on alternatives to certain Chinese suppliers will provide other competitive suppliers growth opportunities in the near-term.

III. Line of Effort Four: Promote Responsible Global Development and Deployment of 5G.

This Line of Effort focuses on how the U.S. Government can lead in 5G development and deployment, support U.S. private sector participation in the standards process, and mitigate risk in the supply chain (among other potential actions). U.S. leadership is essential to realizing the full potential of 5G, both domestically and across the globe. The U.S., along with its allies, should participate in a collaborative effort with the private sector to support the global development of open source and interoperable 5G standards and technology, while at the same time promoting research and development for these technologies. Such efforts will help ensure vendor diversity worldwide, which is critical to the rollout of 5G and future generations of wireless technology in the U.S. and around the world.

Supporting the Development of Open and Interoperable 5G

The global transition to open and interoperable 5G networks has begun. Many of the commercial deployments of open, interoperable network equipment already consider the inclusion of smaller vendors. Further, commercial deployment of Open RAN technologies is expected to ramp up considerably over the next few years. To start, this will likely entail greenfield deployments in areas without congestion and that have relatively low performance demands. Over time, Open RAN technologies will evolve to handle the greater performance requirements needed to serve larger and more concentrated areas.

This nascent shift in network architecture presents a particularly important opportunity for the United States, which has typically led the world in developing innovative software-based

applications.[6] U.S. leadership on 5G should align, however, with the industry's phased approach to 5G deployment, helping to sustain and encourage competition among existing suppliers in the near-term, while encouraging the longer-term transition to Open RAN and open and interoperable 5G networks. Equipment purchases are long-term investments that are costly to replace, so even as operators transition to greater openness, many will continue to use a combination of closed, mixed, and open components for the next few years. For example, AT&T plans to focus on building openness into radio and baseband equipment first, followed by open interfaces in other parts of the network. Meanwhile, newer entrants into this marketplace must develop the manufacturing capacity to deliver their products at scale, to compete effectively with the other large suppliers. Consistent with this phased approach, U.S. policymakers should focus on the following steps going forward.

Facilitate Global 5G Standards and Open Source Software.

Global standards are critical for interoperability among networks and devices. Without technical specifications set by standard-setting bodies, there will be no basis for globally interoperable networks and devices.[7] Continued and enhanced U.S. participation in these efforts, as well as increased coordination at the regional level through the Alliance for Telecommunications Industry Solutions (ATIS), will ensure that technical standards do not favor any single country's preferred technology, and will support the goals of openness and interoperability.

Many standardization efforts are underway, aimed at different aspects of the 5G ecosystem. The leading organization is the 3GPP, with ATIS as the North American Organizational partner, which developed and is continuing to roll out elements of the key 5G New Radio specifications. Equally important are efforts aimed at network openness and interoperability, such as ONAP, the O-RAN Alliance, and the O-RAN Software Community.

[6] James A. Lewis, Sr. Vice President and Director, Technology Policy Program, Center for Strategic International Studies, Statement Before the Senate Committee on Commerce, Science, and Transportation, 5G Supply Chain Security: Threats and Solutions, at 6 (Mar. 4, 2020), https://www.commerce.senate.gov/services/files/563D903B-FEF0-4A1C-9202-A7DC1CCEFC6F.

[7] Patrick Moorhead, *The Crucial Role of Wireless Industry Standards in 5G*, Forbes (Sept. 1, 2017), https://www.forbes.com/sites/patrickmoorhead/2017/09/01/the-crucial-role-of-wireless-industry-standards-in-5g/#626e57ca2cff.

Government support for the open-source architectures and software these entities are developing will be a key to the success of the open ecosystem and the acceleration of innovation.

In addition to promoting interoperability, standards-setting efforts promote critical cybersecurity efforts. For example, 3GPP has a dedicated security working group, and several other standards bodies and organizations — including the Internet Engineering Task Force (IETF), ATIS, European Telecommunications Standards Institute (ETSI), and Counsel for Securing the Digital Economy — are developing 5G security standards. Participation by U.S. industry and academics, and coordination of U.S. positions in ATIS, is essential to ensure the resulting standards support the goals of a robust, competitive supply chain.[8] 3GPP and other bodies work to ensure regional balance and transparency among participating entities, but maintaining that balance requires broad participation.

Government support and partnership in standards setting efforts is equally important. Government should continue to leverage existing processes towards standards like ATIS where it works through ATIS and collaborates with the private sector. Government can also play an important convening role in pulling industry together to determine if there is a need for incentives to continue to participate in standards bodies, to ramp up U.S. private sector representation and determine what those incentives may be (research and development tax credits, direct funding support, etc.). This type of standards support will help solidify U.S. leadership in standards development.

A number of pending legislative proposals would move these efforts forward, as well; the Promoting United States Wireless Leadership Act (H.R. 4500) would encourage trusted companies and wireless stakeholders to participate in standards-setting bodies including the International Telecommunications Union, the 3GPP, the International Organization for Standardization, and other such organizations, and offer technical expertise to facilitate such participation. The Promoting United States International Leadership in 5G Act (H.R. 3763) would establish an interagency working group to enhance U.S. participation in those groups. Implementing and funding these efforts is a critical component of a strategy to maintain U.S. leadership in the 5G ecosystem.

[8] James A. Lewis, *How Will 5G Shape Innovation and Security: A Primer*, Center for Strategic and International Studies, at 7 (Dec. 2018), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf.

Promote Research and Deployment of Open Technologies.

Government's support can not only support existing suppliers, but it can also advance the transition to openness. For example, as open equipment becomes commercially viable, the United States' purchasing requirements should also evolve to follow the example of private carriers that prioritize suppliers committed to open and interoperable networks. For example, the Japanese company Rakuten requires suppliers of new equipment to enable an open radio interface requirement.[9]

The Secure and Trusted Telecommunications Network Act (H.R. 4998), which became law in March 2020, will provide funding to help telecommunications companies purchase new equipment from trusted providers. Reimbursements will be available for both hardware and software, including "virtual communications equipment, application and management software, and services."[10]

Government can also help spur critical research and development that will have global impacts. Although today's dominant suppliers of RAN equipment are based overseas, the U.S. is world leader in many of the technologies necessary for interoperable 5G and software-based networks. Tax-free research and development grants to develop advanced network technologies will help build a base of expertise and a pool of U.S.-based suppliers. Support for core open source software concepts will help create a foundation for innovation and commercialization. Government can also provide financial support for foreign vendors to move research and development operations to the United States and develop solutions for the U.S. market**.**

Supporting Vendor Diversity Worldwide.

The aforementioned efforts government can take to help increase vendor diversity domestically can also have global impact. The U.S. cannot consider these issues in isolation. In order to achieve the scale necessary to ensure the market opportunity for new, innovative solution in the supply chain, these efforts must expand beyond the U.S. Many countries are

[9] Linda Hardesty, *Cisco's Early Bet on RAN Virtualization Propels Altiostar*, FierceWireless (May 6, 2019), https://www.fiercewireless.com/tech/cisco-s-early-bet-ran-virtualization-propels-altiostar.

[10] Secure and Trusted Communications Networks Act of 2019, H.R. 4998, 116th Cong., https://www.congress.gov/116/plaws/publ124/PLAW-116publ124.pdf.

considering today how to address these concerns such as the developments that occurred around the Prague Proposals last year.

We urge government to continue its work with our foreign allies to ensure the market opportunity for existing trusted suppliers and new entrants, which will also help diversify the supply chain. Such commitments are critical to helping to ensure the necessary scale so that existing or new vendors will flourish.

It is also important that government not take steps that would hamper or politicize the standards setting process. There have been some proposals that would arguably place the U.S. Government or entities such as DOD and NIST more actively involved in standards setting as opposed to the traditional means where they work in concert with industry and through established North American standards bodies such as ATIS. It is important for the future of the industry that standards setting bodies remain private sector led.

IV. Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure.

This line of effort focuses on security practices and principles related to 5G and the Security of 5G generally. While there has been much public discussion about the security of 5G, it is important to distinguish between security of 5G and security of the 5G equipment supply chain. While some believe that the 5G's massive IoT and applications at the edge will make networks less secure, the reality is that network virtualization, edge computing power, device management, and automated threat detection and response will create more flexible and secure networks than in any previous generation. Notwithstanding the enhanced security 5G architecture brings, we still face challenges in ensuring a viable, secure, diverse 5G supply chain. With these security nuances in mind, it is critical that government plays a role in both standards development and supply chain resiliency.

Security standards for 5G infrastructure

As discussed above, global standards are critical for interoperability among networks and devices.

In addition to the 5G security specification development well-underway in 3GPP discussed above, work on 5G standards is ongoing at other standards bodies, as well:

- IETF is developing security requirements for network protocols for end-to-end device security. These efforts build on several successful security protocols and standards IETF has developed, such as IP Security, Transport Layer Security, and Simple Authentication and Security Layer.
- ATIS is the North American Organizational Partner to 3GPP and is a forum for North America to discuss and coordinate on specific North American needs. ATIS is driving supply chain and cybersecurity standards for North America, including programs for the 5G Supply Chain; the 5G North American Needs; IoT Device Security; Leveraging Distributed Ledger Technology for ICT Applications; DNS Privacy, Security & Services, ATIS also develops North American/U.S. specific standards, especially for regulatory related topics.
- European Telecommunications Standards Institute (ETSI) is responsible for the standardization of cybersecurity standards internationally and for providing a center of relevant expertise for information and communications technologies, including mobile. The standards include global encryption technologies and algorithms to support integrity, authentication, and privacy.
- Council for Securing the Digital Economy (CSDE), a partnership between global technology, communications, and Internet companies and supported by USTelecom and the Consumer Technology Association (CTA), released a new baseline of security capabilities to improve the security of the Internet of Things (IoT). The Global System for Mobile Communications Association (GSMA), which represents 750 operators with almost 400 companies across the mobile ecosystem worldwide, issued a set of IoT Security Guidelines, and the National Institute of Standards and Technology (NIST) issued a report on Considerations for Managing IoT Cybersecurity and Privacy Risks. U.S. carriers are leading the industry and driving the 3GPP standards organization toward stronger encryption algorithms to enhance the over-the-air interface.

There are also a number of enhancements being defined for 5G within 3GPP security from previous generations of wireless.

- Stronger 3GPP encryption for over-the-air interface to enhance the security between the 5G mobile devices and the 5G network.

- Roaming or network-to-network protection using 5G's new Security Edge Protection Proxy (SEPP) element at the operators roaming border, which will help mitigate against signaling attacks (e.g., SS7, Diameter) when subscribers are roaming between different carriers' networks.
- 5G Subscriber Identity Privacy using a Subscription Concealed Identifier to conceal and protect the 5G Subscription Permanent Identifier, which should help mitigate vulnerabilities to IMSI catchers.
- Increased Home Network Control for Authentication for the 5G home network to verify that the mobile device is present and requesting service from the serving network.
- 5G Unified Authentication Framework to facilitate use of the same authentication methods for both 3GPP (cellular) and non-3GPP (Wi-Fi) access networks.
- 5G Security Anchor Function to facilitate re-authentication of the mobile device when it moves between different access networks or serving networks without having to run the full authentication.

Given the extensive work already underway on security standards, we urge government to avoid imposing security requirements or standards on industry. Continued and enhanced U.S. Government support of and close coordination with industry in the participation in these efforts will help ensure that technical standards do not favor any single country's preferred technology and will further the goal of openness and interoperability. If there are specific requirements for government use cases, government could address those requirements via an RFP or other processes. Additionally, NIST should work to incorporate industry developed standards from bodies like 3GPP and ATIS and adapt them to government use cases. This is already happening at the NIST National Cybersecurity Center of Excellence and we encourage government to continue such efforts.

The standards bodies and processes are iterative and provide a consistent process across generations of wireless. 5G is being built on previous generations of wireless technology and, as a result, in implementing 5G, industry has been able to learn from these past iterations and build in improvements that are addressed via standards. As gaps are recognized, we are able to address those gaps via established standards bodies with new or adapted standards. Now is not

the time for government to disrupt the ongoing global standards process, launch a new standards process, or develop new standards that will not have the benefit of the years of work across generations of wireless that we currently utilize to the benefit of future generations.

Industry is also working with the FCC on security. The FCC Communications, Security and Interoperability Council (CSRIC) VI Working Group 3 on network reliability and security risk reduction issued a report on 5G security in September 2018 and another 5G addendum in December 2018. The current CSRIC VII working group 2 is looking at means to manage security risk in the transition to 5G and working group 3 is looking at methods to manage security risk in emerging 5G implementations. These are extensive reports on 5G security. For example, the 2018 initial report is over 80 pages and details efforts by US players in international standards bodies, as well as the current state of 5G security. It is important that as NTIA considers security, that it does not reinvent the wheel. It should instead continue to leverage processes such as CSRIC that are well under way.

Security requirements/regimes/incentives

In terms of network security, government should recognize the existing business incentives for industry to address security. At AT&T, for example, security is a business imperative and a competitive differentiator. The AT&T Global Network carries more than 350.9 Petabytes of data traffic on an average day, and we take a wide variety of measures to help protect both our network infrastructure and our customers. As more people find themselves working and learning from home during the global pandemic, we have found that our network remains secure, capable, and resilient in the face of skyrocketing demand.

Industry is also actively collaborating on security. As noted, AT&T participates with other carriers in network controls development—which for 5G are outlined extensively in the FCC CSRIC report as well as in the 3GPP and ATIS specifications discussed above.

On the government front, we applaud the work that NIST is doing on device security, as well, such as their dedicated effort to develop a baseline for IoT security. We applaud NIST's differentiation between network and device security. Network security has been primarily addressed through specification development with 3GPP, while device security standards development is the subject of ongoing efforts around the world. We encourage NIST to continue these efforts. In the future, we encourage NIST and other government agencies to expand this

work and collaboration internationally where there are similar efforts ongoing to develop standards around device security (e.g. the European Union Agency for Cybersecurity (ENISA)).

Supporting the well-honed industry approaches to security standards development should be a key tenet to any US plan or strategy concerning 5G. Industry has invested a great deal of time and energy into security standards development with the support of government. We encourage government to foster that work and to help drive adoption of industry standards and approaches to security through procurement policy and government purchasing and use cases. NIST, for example, should work to adapt and apply industry standards to government use cases in 5G security like they do on other cybersecurity issues (e.g. the NIST 800- series of reports).

CONCLUSION

AT&T welcomes NTIAs attention to issues raised in this proceeding and ongoing work surrounding 5G policy and urges continued multistakeholder engagement consistent with the principles provided in these Comments.

Respectfully Submitted,

AT&T Services, Inc.

/s/ Sarah R. Geffroy

Sarah R. Geffroy
David Chorzempa
David Lawson
AT&T Services, Inc.
1120 20th Street NW, Suite 800
Washington, DC 20036
202-457-2121

June 25, 2020