ITI Promoting Innovation Worldwide

Mr. Travis Hall
Telecommunications Policy Specialist
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

June 25, 2020

Re: ITI Comment in Response to NTIA request for public comment on Implementation Plan for National Strategy to Secure 5G; RIN #0660-XC04; Docket No. 200521-0144

Dear Mr. Hall,

The Information Technology Industry Council (ITI) appreciates the opportunity to submit our response to NTIA's request for comment (hereafter "RFC"), on behalf of the Executive Branch, on developing an Implementation Plan for the National Strategy to Secure 5G (hereafter the "5G Strategy Plan").

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises companies that operate in almost every layer of the 5G stack, including semiconductor and network equipment designers and manufacturers, software and digital services companies, as well as those that will harness 5G to evolve their businesses.

We support the USG's increased focus on enabling the deployment of the next generation of cellular network technology; indeed, 5G will be transformative for our society, offering opportunities to U.S. companies and consumers not previously available. We further appreciate the comprehensive nature of the National Strategy to Secure 5G – all four lines of effort can facilitate U.S. leadership in this space.

However, we are also concerned with some of the ways in which Administration officials have proposed ensuring that leadership, including having the government buy controlling stakes in certain companies. In considering how to implement the four lines of effort under the National Strategy to Secure 5G, the USG should ensure in every instance that its actions do not result in picking winners and losers in the 5G marketplace. The private sector should lead, and the market should determine the "winners."

When considering our comments, we encourage the USG to use ITI's *5G Policy Principles* as a foundational document (attached). Recommendations that address many of the questions posed in the RFC are captured there, though in some cases we have expounded upon those principles in our response.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Immediately below, we offer a summary of our recommendations, followed by answers to each of the questions posed in the RFC.

Summary Recommendations

The U.S. government should take steps to enable an environment that supports innovation and encourages investment in the foundational and new technologies that will facilitate 5G networks. These steps should include prioritizing freeing up additional spectrum, promoting internationally harmonized spectrum bands as appropriate, using targeted government/public funding to complement private sector investment to accelerate the rollout of 5G infrastructure, investing in workforce training, and further streamlining siting requirements.

The U.S. government should take a risk-based approach to 5G security, including focusing on threats to the 5G ecosystem beyond those associated with supply chain. We recommend that policymakers take a risk-based approach to 5G security, ensuring that any effort is evidence-based and fit-for-purpose. Policymakers should consider how to address the full range of risks as a singular focus on equipment and suppliers threatens to stifle what should be strong national attention on the full breadth of 5G security issues.

The U.S. government should continue efforts to lead in global conversations happening on 5G. This should include continuing multilateral and bilateral engagements, creating the multilateral fund set forth in several pieces of legislation, considering carving out a national security exception for telecommunications networks in Development Finance Corporation (DFC) funding, reconsidering the content rules that currently govern Export Import Bank transactions, and continuing and expanding funding for 5G- and cybersecurity-related business development trade missions, reverse trade missions, and other events.

The U.S. government should seek to support increased U.S. industry participation in standards bodies working on 5G specifications, through supporting industry-led bodies with transparent, rules-based processes, making the United States a more attractive meeting location for standards development organizations (SDOs) to host meetings, ensuring that current and future policies and regulations do not unintentionally inhibit U.S. company participation in international standards bodies, reexamining NISTIR 8074 to see whether and how recommendations are applicable to 5G work, and regularly communicating with U.S. industry.

Finally, the U.S. government should work closely with industry partners on all facets of the Implementation Plan. We appreciate the opportunity to provide comments in response to this RFC and encourage the U.S. government to maintain consistent engagement with industry on all aspects of the Implementation Plan. It is imperative that the U.S. government collaborate with industry, as secure 5G deployment will only succeed with sustained effort from all stakeholders.

Line of Effort 1: Facilitate Domestic 5G Rollout

1) *How can the United States (U.S.) Government best facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem (e.g., equipment manufacturers, chip manufacturers, software developers, cloud providers, system integrators, network providers)?*

The basis for sound 5G policy rests on ensuring an environment that supports innovation and encourages investment in the foundational and new technologies that will facilitate the next generation of networks, while also driving deployment by freeing up spectrum and taking steps to make 5G deployment easier. As we lay out in our policy principles, we recommend that the USG:

- **Prioritize freeing up additional spectrum for 5G.** ITI supports increasing both commercial and private access to licensed, unlicensed, and shared spectrum for 5G, particularly in the mid- and high-bands.
- **Promote internationally harmonized spectrum bands, as appropriate.** Policymakers should pursue opportunities for global harmonization of spectrum bands, while maintaining individual countries' sovereignty to allocate spectrum for domestic use.
- **Use targeted government/public funding to complement private sector investment and accelerate the rollout of 5G infrastructure.** Where public funding is available and utilizable, it should facilitate solutions that are based on open, interoperable approaches, and be made available for 5G infrastructure and services, as well as for 5G operating expenses. Additionally, we note that leading-edge semiconductor innovations are key components of the transition to 5G networks and similar funding mechanisms—whether through investment tax credits or federal and state grant programs—should be extended to include the purchase of semiconductor manufacturing equipment and semiconductor manufacturing facility investment expenditures.
- **Invest in workforce training.** In addition to the tower technicians and telecom crews servicing 5G infrastructure, 5G will also require more datacenter technicians, cloud systems administrators, cybersecurity experts and other workers with the skills to advance virtualization. Governments should prioritize funding training and retraining for workers to meet 5G-related workforce needs. This training and retraining should be conducted in conjunction with industry to ensure that it meets the required skillset and policymakers should consider providing incentives to industry to support training.
- **Further streamline siting requirements.** Governments at all levels should consider siting reforms, including streamlining licensing requirements to speed up the deployment of 5G infrastructure. The FCC should continue to remove barriers to 5G siting, considering not only how to facilitate new small cell technology but also how to upgrade existing cell sites.

2) *How can the U.S. Government best foster and promote the research, development, testing, and evaluation of new technologies and architectures?*

It is important that the USG consider market-based solutions to counterbalance immense financing and subsidization available to global competitors. The USG should also be mindful and coordinated to avoid policies that create undue financial burdens on companies and cause them to divert money from R&D to undue costs (e.g. tariffs). Funding for research and development is a hugely important factor in maintaining a consistent edge in network technology.

To foster innovation in 5G technologies, the U.S. Government should consider opportunities for public-private partnerships, cooperative agreements, and grant agreements to support ongoing research and development. Public-private partnerships are an important tool for the Government to facilitate not only the technical investment in 5G, but also the legal and policy framework to support and govern the technology long-term. Historically, public-private partnerships have helped bring to fruition large-scale projects by combining private sector technology and innovation with

public sector oversight and buy-in; both are critical requirements for advancing a cohesive national 5G strategy.

Cooperative agreements and federal grants are two other mechanisms to channel federal funding toward 5G research, development, and testing in a streamlined manner. These flexible instruments are not subject to the Federal Acquisition Regulation (FAR), and can potentially expand the universe of private companies willing to partner with the federal government for research and development activities related to 5G. Legislatively, Congress should consider incentivizing 5G investments by expanding federal agencies' existing grant authorities and funds, while still ensuring federal government oversight of critical projects to maintain compliance with applicable legal requirements.

To this end, the U.S. government should also seek to support foundational semiconductor research, development, and manufacturing as part of its overall strategy to grow a strong 5G ecosystem. Continued advancements in semiconductor technology will be critical in driving advancements in 5G technology and should not be overlooked as the USG seeks to develop the National Strategy to Secure 5G Implementation Plan.

3) *What steps can the U.S. Government take to further motivate the domestic-based 5G commercial ecosystem to increase 5G research, development, and testing?*

Many federal agencies have existing legal and procurement authorities to support private sector research and development (R&D) work for agencies' procurement and adoption of mission-critical technologies like 5G. By investing R&D funds through contracts or other instruments (e.g. Other Transaction Authority agreements), the Government can incentivize private sector investment in 5G by providing seed funding for prototype projects, and help reduce barriers that agencies have to confront in purchasing private sector developed cutting edge solutions. This arrangement is also advantageous for private sector companies, as the technical risk is shared between the Government and the contractor.

Successful R&D prototypes generally move on to the testing phase and the Government's security accreditation process. This is beneficial for private sector companies as the Government shares responsibility for ensuring compliance with security protocols and standards. Technologies that meet Government technical and security requirements can move more quickly toward wide-spread Government adoption through subsequent procurements, which acts a further incentive for companies to participate in Government-sponsored R&D for emerging technologies like 5G.

4) *What areas of research and development should the U.S. Government prioritize to achieve and maintain U.S. leadership in 5G? How can the U.S. Government create an environment that encourages private sector investment in 5G technologies and beyond? If possible, identify specific goals that the U.S. Government should pursue as part of its research, development, and testing strategy.*

As we reference in several areas throughout our comments, we support the continued prioritization by the U.S. Government of R&D into areas foundational to next generation wireless technologies. We advocate for increased R&D in areas including increased funding for the highly technical USG labs such as those at the DoD, DoE, NIST, etc. into key foundational and applied research areas to bring USG R&D spending closer to par with the 5G investments made by competitors, as well as other important telecommunications R&D efforts, such as in the area of broadband funding. In particular, we recommend that the USG elevate R&D related to virtualized

architectures and software-defined networking, two areas where the United States can leverage existing technological prowess in other contexts to increase competitiveness in 5G.

We also recommend that the USG prioritize and increase R&D spending for 5G use cases, including those related to the Internet of Things (IoT) and Artificial Intelligence (AI), as well as advanced semiconductors that will underpin such technologies. Investments in 5G infrastructure and next generation applications are absolutely imperative in fueling a cycle of investment and innovation. As more consumers and businesses harness 5G, application developers are incentivized to create innovative new offerings. From there, these new applications and use cases drive demand for 5G enabled devices and connections, thereby encouraging further investment in 5G infrastructure. Examples of R&D and pilot projects that could harness 5G built on open and interoperable infrastructure include innovations in energy monitoring on the power grid, smart network monitoring in commercial facilities that require a high degree of government regulation and security. The USG should also provide funding for cloud testbeds developed in partnership with U.S. operators to create opportunities for stakeholders to create, test, and deploy new use cases for 5G. It may also be helpful for the USG to consider allocating funding for 6G advanced research.

Finally, we recommend that the USG support research to apply risk-based and standards-based approaches to improve security of advanced communication networks in critical infrastructures.

Line of Effort 2: Assess Risks to and Identify Core Security Principles of 5G Infrastructure

1) *What factors should the U.S. Government consider in the development of core security principles for 5G infrastructure?*

In ITI's 5G Policy Principles, we provide recommendations for policymakers to consider in developing measures to address challenges related to 5G security. We believe these principles can inform the USG's development of core security principles.

- **5G security-related policies should take a risk-based approach.** Any policy intended to address challenges related to 5G security should be risk-based, evidence-based, adaptable, and fit-for-purpose. To the extent that governments continue to focus on supply chain security in the context of 5G deployment, they should either undertake or promote risk assessments to gain fuller visibility into the threat landscape, including the supply chain ecosystem and which risks can be mitigated and which ones cannot. Policies should promote the procurement of equipment from trusted suppliers that adhere to international standards, consider geopolitical implications of manufacturing locations, and encourage diverse supply chains to help reduce risk. Policies should also include a focus on breaking down barriers to trade in technology in order to help with diversification.
- **Policymakers should focus on threats to the 5G ecosystem beyond those associated with specific supply chain actors and equipment.** While we encourage governments to continue to focus on supply chain risk management, supply chain is only one of the many important 5G risk factors. An exclusive focus on concerns regarding particular suppliers will compromise demonstrative progress towards securing 5G. Instead, policymakers should consider adopting policies that seek to manage the full range of security risks to mobile network infrastructures, applications, and services, including devices and data. For

instance, automated and distributed threats such as botnets will likely be a more pervasive issue in the context of 5G network deployment, and policymakers should consider innovative cybersecurity solutions to adequately mitigate such threats, including through the use of AI and other automated tools. As the U.S. Department of Homeland Security recommended in its Overview of Risks Introduced by 5G Adoption in the United States, "the U.S. Government and industry partners can develop security capabilities that protect not only the 5G infrastructure, but also the applications and services that utilize it. The U.S. Government can do this by incorporating a prevention-focused approach that focuses on visibility and security across the mobile network."[1] Further, a singular focus on equipment alone threatens to stifle what should be strong national attention in all countries on the full breadth of cybersecurity risk factors facing 5G networks.

- **Government and industry must share responsibilities and collaborate.** Government and industry share the goals of mitigating cybersecurity threats to mobile and 5G network infrastructure, preventing cyberattacks, and reducing the impact of related cybercrime. As in all areas of cybersecurity, achieving these goals is a collective effort. Public-private partnerships should be leveraged to ensure that we arrive at the desired policy outcome of more secure 5G networks.

2) *What factors should the U.S. Government consider when evaluating the trustworthiness or potential security gaps in U.S. 5G infrastructure, including the 5G infrastructure supply chain? What are the gaps?*

As an overarching matter, we would like to emphasize our support for viewing issues of 5G equipment or infrastructure security through the lens of "trustworthiness," which has many dimensions, rather than solely through the lens of country-of-origin. While country-of-origin is one risk factor to be considered, it is not the sole and dispositive factor. Indeed, after a year of study the Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force working group on Threat Assessment catalogued 188 supplier related threats. While one of these factors was appropriately the country of origin of a supplier, it would be a mistake to not take a holistic view of the 5G threat and risk landscape when evaluating the trustworthiness of 5G equipment. In fact, the practices of a vendor-- how securely a vendor develops its products and services within a wider culture of security and recognized development best practices -— should be the priority and focus. This is a better indicator of the security of products/services than looking just at the product/service itself. The work of the ICT SCRM Task Force has made many recommendations regarding good practices and how to incentivize vendors to adopt these practices.

Additionally, we fully support the Prague Proposals[2] and we recommend that the USG continue to leverage them as a starting point in understanding relevant risk assessment criteria. Utilizing the Prague Proposals as a foundation for policymaking can further promote procurement of equipment from trustworthy suppliers.

Beyond that, when evaluating trustworthiness, we recommend that the U.S. government consider the geopolitical implications of manufacturing locations, adherence to international standards, the

[1] https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf

[2] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

risk management processes that a company or supplier is undertaking, and the other supply chain threat vectors identified by the Task Force.[3] As mentioned above, this working group's supplier threat assessment identified country-of-origin as *one* threat out of 188 potential factors to take into consideration.[4] We believe this assessment is a useful tool for policymakers and industry alike to understand the full range of threats that may impact a supplier and that can help to inform trustworthiness evaluations.

Another important point to make is that security is not static, so the notion of filling "gaps" is perhaps not ideal. 5G infrastructure risk management will be a continuous process of assessing changing threats and adapting to new technologies. Government direction to focus too much on one element may actually divert resources from safeguarding the broader technology ecosystem. Companies must be able to manage their systems based on evolving priorities and circumstances. That is why a focus on risk management processes in the context of 5G security is so important.

3) *What constitutes a useful and verifiable security control regime? What role should security requirements play, and what mechanisms can be used to ensure these security requirements are adopted?*

We generally advocate for voluntary, flexible frameworks when it comes to security requirements, especially because security is not static and any regime needs to be adaptable. It is our view that a useful and verifiable security control regime should be voluntary, flexible, and able to adapt to different risks as they emerge. We suggest that any mechanism considered should be voluntary and industry-driven.

4) *Are there stakeholder-driven approaches that the U.S. Government should consider to promote adoption of policies, requirements, guidelines, and procurement strategies necessary to establish secure, effective, and reliable 5G infrastructure?*

The ICT SCRM Task Force is a private sector and government stakeholder-driven group that the USG should continue to leverage when implementing the National Plan to Secure 5G. Indeed, the ICT SCRM Task Force brings together government and private sector participants to effectively identify, prioritize, and mitigate ICT supply chain risks – which include 5G security risks as a subset -- with the goal of providing realistic, actionable, timely, economically feasible and risk-based recommendations for addressing those risks.

It is also worth highlighting the importance of continuing to support industry-led SDOs, which are developing many of the technical specifications, including those related to security, that will support 5G networks. See our response in 4.2 for additional recommendations as to how to support private sector participation.

5) *Is there a need for incentives to address security gaps in 5G infrastructure? If so, what types of incentives should the U.S. Government consider in addressing these gaps? Are there incentive models that have proven successful that could be applied to 5G infrastructure security?*

[3] https://www.cisa.gov/publication/ict-scrm-task-force-interim-report
[4] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf

The SECURE Technology Act (P.L. 115-390), though not yet fully implemented, requires that the Federal Acquisition Security Council, established under the Act, identify best practices, legislative and regulatory policy changes for securing cyber supply chains and recommend policies to incentivize their adoption by industry in its Strategic Plan. Product security assurance practices, based on recognized international standards such as ISO/IEC 29147:2018 (vulnerability disclosure), ISO/IEC 30111:2019 (vulnerability handling), and the FIRST PSIRT Services Framework (incident response), are examples of best practices that industry partners should be encouraged to adopt. In alignment with the work being undertaken by the ICT SCRM Task Force referenced above, the U.S. government could explore incentives such as procurement preference, via Qualified Bidder/Manufacturer Lists, for vendors who follow such best practices.

Line of Effort 3: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide

Economic and national security are very closely linked. As we note in our *National Security Principles*[5], it has never been more important for the U.S. government and industry to work together to harness U.S. technological leadership, economic openness, and international engagement to strengthen national security.

1) *What opportunities does the deployment of 5G networks worldwide create for U.S. companies?*

The deployment of 5G globally presents enormous opportunity for U.S. companies, particularly as 5G technology is expected to enable $13.2 trillion in economic output by 2035.[6] 5G use cases are expected to generate tremendous economic growth – the increased speed, capacity, and functionality of 5G networks will help to enable the next generation of data-enabled innovations such as IoT and AI.

As countries around the world deploy 5G, U.S. companies can seize upon these new networks to implement use cases that were previously unachievable. Beyond that, encouraging open and interoperable solutions in the deployment of 5G networks will ensure that different vendors can supply different aspects of the 5G network, allowing U.S. companies the opportunity to better compete.

2) *How can the U.S. Government best address the economic and national security risks presented by the use of 5G worldwide?*

We recommend that the USG reference our recently released *National Security Principles*, which offer guidance to U.S. policymakers on how to best approach both economic and national security risks while maintaining its technological leadership, economic openness, and strong alliances. These are applicable across a broad swath of technology areas, including 5G. As a foundational matter,

[5] https://www.itic.org/policy/ITI_NationalSecurity_Policy_June2020.pdf

[6] https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study-2019.pdf

strong national security requires maintaining technological leadership in a variety of areas. Our recommendations in response to Line of Effort 1 address some ways in which the United States Government can help to support U.S. technological leadership.

The USG should also seek to advance trade and investment policies that allow companies to succeed commercially, thereby contributing to the technological leadership and economic competitiveness that is so vital to strengthening U.S. national security. We offer some ideas for this in response to questions under Line of Effort 4.

The USG should also ensure that any approach it takes is targeted at identifiable national security risks, thus avoiding overly broad policy responses that may have negative impacts on U.S. competitiveness, the United States' relationship with allies, and the USG's ability to procure 5G technology.

Finally, given the constant cross-border flow of goods, services, and data, we recommend that the USG closely coordinate its technology-related national security policies with like-minded economies, avoiding harmful policy fragmentation and maximize the likelihood of achieving shared security objectives.

3) *How should the U.S. Government best promote 5G vendor diversity and foster market competition?*

We appreciate the interest that the USG has taken in examining the role that open radio access networks can play in promoting vendor diversity and fostering market competition. We believe that all governments, including the USG, should support open and interoperable solutions for 5G networks, which will allow for interoperability, supplier diversity, competitiveness, and innovation on a massive scale. Indeed, leveraging open and interoperable solutions can help to avoid vendor lock-in. We therefore encourage the USG to adopt policies that promote the use of open 5G architectures.

In particular, we support the language used in Sec. 501 of the Intelligence Authorization Act for FY2021, which would create a Communications Technology Security and Innovation Fund to help spur innovation in open, software-based wireless technologies, an area where the United States could be very competitive.

4) *What incentives and other policy options may best close or narrow any security gaps and ensure the economic viability of the United States domestic industrial base, including research and development in critical technologies and workforce development in 5G and beyond?*

Please refer to our responses to questions posed under Lines of Effort 1 and 2, which we believe sufficiently address the question asked here.

Line of Effort 4: Promote Responsible Global Development and Deployment of 5G

1) *How can the U.S. Government best lead the responsible international development and deployment of 5G technology and promote the availability of secure and reliable equipment and services in the market?*

We appreciate the efforts the USG has undertaken to promote responsible international development and deployment of 5G technology thus far. We have several specific recommendations to offer when considering how to continue with these efforts, including:

- **Create the Multilateral Telecommunications Security Fund as proposed in Sec. 501 of the Intelligence Authorization Act for FY 2021.** In addition to setting up other helpful funding mechanisms noted elsewhere in our response, the language set forth in the Act would create a Multilateral Telecommunications Security Fund. We are supportive of this fund, as it would provide additional direct support to the United States in its engagements with foreign partners.
- **Carve out a national security exception for telecommunications networks in Development Finance Corporation (DFC) funding.** While 5G is rightfully a top priority for the DFC, there are currently constraints on where it can operate. The European Energy Security and Diversification Act of 2019 (P.L. 116-94, Div. P, Title XX) eases DFC's less-developed country requirement for energy infrastructure projects in Europe and Eurasia. This authority for energy projects, which provides commercial opportunities in upper-middle-income countries that may have both strategic and development benefits, should be extended globally for deployment of secure and trusted telecommunications infrastructure.
- **Reconsider the content rules that currently govern Export Import Bank (Ex-Im) transactions as they are not necessarily applicable to the tech sector.** Indeed, current U.S. content requirements hinder the ability of Ex-Im to support the deployment of trusted network equipment overseas. Especially in the tech sector, IP and R&D may be U.S.-based, even if the *product* is manufactured elsewhere. This important aspect is not considered in the current iteration of U.S. content requirements that dictate whether Ex-Im can support an overseas deal, therefore making it significantly more difficult for Ex-Im to support deals related to 5G technology.
- **Continue advocacy through bilateral and multilateral dialogues, including the Digital Connectivity and Cybersecurity Partnership Program and Prague Conference.** We encourage the USG to continue consistent engagement on this issue through bilateral and multilateral dialogues, engaging with other countries wherever possible. That said, we encourage the USG to consider how to creatively advocate for secure equipment and services, especially in countries where cost is a significant driver in decision-making. Different arguments may be more effective in different places. In any engagement with foreign countries, we encourage USG to work closely with industry representatives, who can oftentimes present unique and persuasive perspectives on issue areas related to 5G deployment.
- **Continue and expand funding for 5G- and cybersecurity-related business development trade missions, reverse trade missions, and other events led by the U.S. Trade and Development Agency (USTDA), U.S. Agency for International Development (USAID), and U.S. Department of Commerce.** These agencies regularly organize opportunities for U.S. companies to identify business opportunities and potential customers in foreign markets for U.S. technologies. The breadth of missions and events focused on 5G/mobile security/ cybersecurity has increased in recent years, largely due to growing demand. Although many in-person missions/events have been put on hold due to the Covid-19 pandemic, they should be resumed as soon as practicable, and they should be expanded in terms of regularity and participating countries. During the current crisis, these agencies should determine ways to hold these missions/events virtually.

2) *How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies?*

As we state in our *5G Policy Principles* and earlier in our response, standards are an incredibly important driver and enabler of 5G technology. We appreciate that the USG recognizes this and is considering how to encourage and support U.S. private sector participation in standards development, consistent with longstanding US government policy and the law. Below are specific recommendations that the USG can undertake to best incentivize and support U.S. industry participation:

- **Support industry-led bodies with transparent, well-understood rules-based processes in place.** Companies that seek to compete in 5G technologies must participate in international standards development processes, and they must not be restricted in their decisions to choose which bodies are best suited for their specific work. The U.S. government should continue to support participation in industry-led bodies with transparent, rules-based processes in place. The U.S. government should also encourage other nations to rely on and reference international standards in relevant policies and regulations.
- **Make the United States a more attractive meeting location for SDOs to host meetings.** Attending standards meetings typically requires a significant amount of travel and time commitment, making the U.S. a more appealing meeting locale for those based in the U.S. The U.S. government can encourage this by facilitating visa applications for foreign standards experts to routinely attend meetings in the United States. The inability to get U.S. visas on time has often proved an impediment to hosting meetings in the United States.
- **Ensure that current and future policies and regulations do not unintentionally inhibit U.S. company participation in international standards.** For example, the May 2019 entity list designation of Huawei and the associated Temporary General License created an unfortunate situation in which U.S. companies were precluded from participating in technology-related SDOs in which Huawei or other listed entities were also a participant. It also adversely affected standards development activities in some US-headquartered standards and specifications developing organizations.
- **Reexamine NISTIR 8074: Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives to Cybersecurity[7] and see whether and how the recommendations included in that report are applicable to 5G.** NIST published a comprehensive report in 2015, which set out proposed USG strategic objectives for pursuing and developing international standards related to cybersecurity and provides a series of recommendations for doing so. We believe that the strategic objectives set out in this document are similarly applicable to 5G standards. It would be helpful for the USG to reference this document and consider which recommendations may be applicable to help achieve these strategic objectives in the context of 5G.
- **Engage in regular communications with U.S. stakeholders.** The U.S. government and the private sector should regularly engage outside of standards development activities. Consistent engagement helps ensure that all government and U.S. private sector stakeholders are aware of standards-related activities. This exchange creates mutual understanding of progress, concerns, and strategies, along with clarifying any

[7] https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf

misunderstandings about ongoing efforts. ITI has sought to convene public-private sector standards roundtables to periodically bring stakeholders together and would be eager to work with the U.S. government to regularize such meetings.

Further, while we understand the desire to send diplomats and other US government staff to track standards activities, technical subject matter expertise is critical to fulsome engagement in standards meetings, which are highly technical meritocracies. At the same time, there often is a gap between policy generalists and technical experts, so creating regular opportunities for the two to engage is important to developing a strategic plan to approach to these issues.

3) *What tools or approaches could be used to mitigate risk from other countries' 5G infrastructure? How should the U.S. Government measure success in this activity?*

We understand and acknowledge that the USG is appropriately focused on national security risks related to the global 5G networking buildout, and that the USG has made judgments regarding the use or deployment of 5G equipment in U.S. networks. However, we also note that other countries appear to have reached different conclusions regarding security risks posed by their 5G infrastructure, including whether and how such risks can be mitigated. We recommend the USG continue to engage with international partners to better understand their approach to mitigating such risks, and factor this into its own risk-based analyses of other countries' 5G infrastructures.

In seeking to mitigate risk that may stem from other countries' 5G networks, the USG should avoid overly broad policy responses, which can often result in unintended consequences that pose an even greater risk to national or economic security. For example, consider Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which prohibits government agencies from contracting with entities that "use" equipment from covered Chinese entities in their supply chains. While the national security objective of this law is well-intentioned, this overbroad provision will drastically impede the USG's ability to purchase equipment from leading trusted tech companies. Even if companies do not integrate covered equipment into their own products, it is often impossible for companies to have full visibility into all equipment used at all levels of their supply chain, especially considering that many downstream business transactions do not have formal contractual relationships. Thus, many innovative companies will find it difficult to certify compliance with the law at all supplier tiers and may have to consider exiting the US federal market. While this policy has not come into effect yet, we caution against similar overly broad policy responses that may create unintended consequences to U.S. technology competitiveness.

It is therefore important that the USG encourage and participate in information-sharing between stakeholders to gain a full picture of the risk landscape, potential mitigations, and potential downstream ramifications of policies intended to address those risks. For example, although we understand that the State Department is still collecting responses to its "5G Clean Path" RFI, the goal it is intended to achieve -- to assist the USG in identifying approaches to secure 5G networks and mitigate risks associated with other countries' 5G infrastructure – appears to be an approach worth exploring.

4) *Are there market or other incentives the U.S. Government should promote or foster to encourage international cooperation around secure and trusted 5G infrastructure deployment?*

The United States should endeavor to increase its competitiveness as a global investment destination. In addition to providing incentives through investment tax credits and grant programs related to the 5G technology ecosystem, the United States should continue efforts to strengthen trade and investment relationships with allies, partners, and economies around the world. Such efforts would be well-received and will complement efforts to strengthen international cooperation around secure and trusted 5G deployment.

5) *Both the Department of Commerce and the Federal Communications Commission (FCC) have rulemakings underway to address the security of the telecommunications infrastructure supply chain. Are there other models that identify and manage risks that might be valuable to consider?*

We recommend that the USG consider a similar approach to that which the EU has taken in developing the EU 5G Security Toolbox.[8] Before releasing the 5G Security Toolbox in January 2020, the EU consulted with all Member States regarding an EU-wide joint risk assessment for the 5G rollout followed by a 5G threat landscape report. The EU 5G Security Toolbox was developed by a group of public and private sector experts to facilitate an EU-wide vision for managing cybersecurity risks of 5G.

The EU 5G Security Toolbox lays out strategic measures, technical measures, and supporting actions to address nine risk categories. Member States can prioritize risks according to their risk assessments and select the corresponding measures and mitigation plans that suit their needs. We recommend the USG look at this model, which could be helpful in identifying and managing risks related to 5G. That said, there are areas of the Toolbox that could be improved, specifically with regard to adding additional recognized cybersecurity best practices that are necessary to counter the sophisticated, automated nature of cybersecurity adversaries.

With respect to the Department of Commerce rulemaking referenced here, we refer NTIA to our comments submitted in response to the Commerce Department's NPRM.[9] We reiterate here that any approach taken to secure the ICTS supply chain should be risk-based, evidence-based, narrowly scoped, and tied to the specific national security criteria outlined in the associated Executive Order. We also stress that the current rule as drafted is far too vague to be practically implementable and given the breadth and scope, serves to undermine all information and communications technology and services transactions with any nexus to the United States. We therefore recommend that any future iteration of this rulemaking: ensure that it advances U.S. national security interests without putting American competitiveness at risk or eroding trust in U.S. businesses; address identifiable, material concrete security risks for a narrow subset of ICTS elements; provide clear guidance to industry by including parameters and criteria for a fair, workable, repeatable process that Commerce will use when evaluating a transaction; and be guided by existing taxonomies, amongst other suggested improvements as noted in the above-referenced submission.

[8] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[9] https://www.itic.org/dotAsset/d6447508-0425-4848-b968-4f91490b8494.pdf

6) *What other actions should the U.S. Government take to fulfill the policy goals outlined in the Act and the Strategy?*

We cannot overemphasize the importance of a coordinated, whole-of-government approach to supporting the deployment of 5G in the United States and globally. In the United States, too often there are a host of agencies working on different initiatives, sometimes duplicating efforts. We appreciated the USG's efforts to appoint a "5G Czar" in charge of coordinating all ongoing efforts related to 5G. However, with his recent transition to a new role, we would encourage the Administration to consider appointing a new office (or person) to lead 5G-related efforts.

Once again, ITI appreciates the opportunity to submit comments to this RFC. We believe that the United States has an enormous opportunity to lead in secure 5G deployment both at home and abroad. We hope that our comments will be helpful in guiding the White House as it seeks to develop an Implementation Plan for the National Strategy to Secure 5G.

Sincerely,

John S. Miller
Senior Vice President of Policy
and Senior Counsel

Courtney Lang
Director of Policy

ITI's 5G Policy Principles and 5G Essentials for Global Policymakers

June 2020

ITI
Promoting Innovation Worldwide

Globally, the deployment of next generation communication networks has been an area of significant focus for policymakers. This increased attention is warranted, especially given the promise that 5G technology holds for innovation, from precision agriculture to advances in telemedicine to the realized vision of smart cities.

5G will also have a tremendous economic impact. By one estimate, globally, 5G technology is expected to enable $13.2 trillion in economic output by 2035.[1] In the United States alone, 5G is expected to generate up to $275 billion in infrastructure investment, thus creating approximately three million new jobs and boosting GDP by $500 billion annually.[2]

Beyond infrastructure investment, the use cases for 5G are projected to generate significant economic growth. In particular, the increased speed, capacity, and functionality of 5G networks will help to enable the next generation of data-enabled innovations such as the Internet of Things (IoT) and artificial intelligence (AI).

5G networks will enable increased speeds and staggering amounts of data – mobile traffic is expected to grow by a factor of 4 from 38 exabytes in 2019 to 160 exabytes per month in 2025 (exabyte = one billion gigabytes).[3] The implications of these numbers are significant not only because 5G will power the next wave of data-driven innovations, but also because of implications for individual privacy, national security, technological leadership, and economic competitiveness.

Thus, with the promise of 5G comes a host of policy opportunities and challenges that policymakers worldwide need to balance. As the premier technology trade association with a presence across the globe, ITI represents the full spectrum of technology companies, including those contributing to nearly every facet of 5G, from the equipment at the core to the applications that will run on top of 5G networks.

It is through this lens that ITI and its member companies have developed our 5G Policy Principles, a set of recommendations to help guide policymakers as they develop measures to advance this critical technology globally and our 5G Essentials for Global Policymakers, an informative tool that policymakers, industry partners, and other stakeholders can use to understand the policy recommendations that we set forth.

[1] https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study-2019.pdf
[2] https://www.accenture.com/_acnmedia/pdf-82/accenture-strategy-accelerating-future-economic-value-2018-pov.pdf
[3] https://www.ericsson.com/en/mobility-report/reports/november-2019/mobile-data-traffic-outlook

ITI's 5G Policy Principles for Global Policymakers

As the premier technology trade association with a presence across the globe, ITI represents the full spectrum of technology companies, including those contributing to nearly every facet of 5G, from the equipment at the core of 5G to the applications that will run on top of 5G networks.

As policymakers seek to promote 5G deployment, there are four key areas where sound policy approaches and government action are essential: Innovation and Investment; Deployment and Access to Spectrum; Security; and Standards.

Using these key areas, we developed a roadmap to help policymakers as they develop measures to advance this critical technology across the globe.

We encourage policymakers to take a holistic approach and consider measures that take into account principles from every area, as 5G cannot be deployed effectively otherwise.

1 Innovation and Investment

The basis for sound 5G policy rests on ensuring an environment that supports innovation and encourages investment in the foundational and new technologies that will facilitate the next generation of networks. Governments should consider a full range of policy options in order to support innovation, enable market competition, ensure a skilled workforce, and harness the transformative power of 5G.

- **Incentivize private and public sector investments in 5G research and development (R&D).** 5G R&D is important both for creating new technologies and in supporting standards development. Leaders in technological development are best positioned to be leaders in standards development. This starts with robust investment in R&D and developing technical experts with the knowledge and skills to effectively engage in standards development. Governments should incentivize private sector investments in 5G R&D, increase public funding for 5G and foundational technology R&D, and take steps to remove regulatory or market access barriers that can force companies to redirect funding from R&D to compliance issues.
- **Support open and interoperable solutions for 5G networks.** Supporting the development of 5G networks built on open standards will allow for interoperability, supplier diversity, competitiveness, user choice, and innovation on a massive scale. Examples include equipment developed pursuant to the standards set forth by organizations such as the O-RAN Alliance, the Telecom Infra Project, 3GPP, the O-RAN Software Community, or any successor organizations. We encourage governments to adopt policies that promote R&D funding for open 5G architectures.
- **Invest in workforce training.** In addition to the tower technicians and telecom crews servicing 5G infrastructure, 5G will also require more datacenter technicians, cloud systems administrators, cybersecurity experts and other workers with the skills to advance virtualization. Governments should prioritize funding training and retraining for workers to prepare for and meet 5G-related workforce needs. This training and retraining should be conducted in conjunction with industry to ensure that it meets the required skillset. Policymakers should consider providing incentives to industry to support training.
- **Ensure the free flow of data across borders.** To fully realize the benefits of 5G – particularly the role 5G will play in further enabling AI and other data-driven innovations – governments need to ensure that data and metadata can move freely across borders. As such, we encourage governments to strengthen their commitment to facilitating the free flow of data across borders and refrain from imposing localization measures requiring the local storage or processing of data, or the use of local computer facilities.

2 Enabling 5G Deployment and Access to Spectrum

Governments should also work to free up spectrum – oftentimes characterized as the lifeblood of wireless networks – and take steps to streamline 5G deployment.

- ✔ **Prioritize freeing up additional spectrum for 5G.** ITI supports increasing both commercial and private access to licensed, unlicensed, and shared spectrum for 5G, particularly in the mid- and high-bands.
- ✔ **Promote internationally harmonized spectrum bands.** Policymakers should pursue opportunities for global harmonization of spectrum bands, while maintaining individual countries' sovereignty to allocate spectrum for domestic use.
- ✔ **Use targeted government/public funding to complement private sector investment and accelerate the rollout of 5G infrastructure.** Ensuring ubiquitous access to connectivity should be a goal for policymakers everywhere, as they have an important role to play by incentivizing the expansion of 5G to rural and hard-to-serve areas where a business case can be hard to make. Where public funding is available and utilizable, governments should avoid using such funding to overbuild and instead prioritize areas that would be otherwise unserved by private sector investments. Government funding should facilitate solutions that are based on open, interoperable approaches grounded in international standards, and be made available for 5G infrastructure, services, and operating expenses.
- ✔ **Governments at all levels should consider local siting and licensing reforms to speed up the deployment of 5G infrastructure.** In many places, governments have legacy permitting and siting regulations for wireless infrastructure which were designed with previous generations of technology in mind. 5G deployment will rely heavily on small cells, not the large, new cell towers for which existing regulatory regimes were designed. Governments should adopt deadlines for regulatory reviews and reasonable fee structures, as well as changes to permitting processes to speed deployment of fiber as a transport media capable of scaling to the demands of 5G.

3 Security

Cyber threats continue to impact network infrastructure, applications, and services, as well as customers/end-users, such as consumers and enterprises. These risks will grow with the scale enabled by 5G: dramatically increased network capacity and speed coupled with more connected devices will create more potential opportunities for compromise. Emerging threats may pose a danger not just to 5G networks but to connected ecosystem players, including, for example, critical infrastructure or services like energy, manufacturing, utilities and other industry sectors connected via 5G. Government policymakers are appropriately prioritizing the security of 5G networks and should consider the points below:

- **5G-related security policies should be risk-based.** Any policy intended to address challenges related to 5G security, including supply chain security, should be risk-based, evidence-based, adaptable, and fit-for-purpose – i.e., such policies should address concrete, identifiable security risks. To the extent that governments continue to focus on supply chain security in the context of 5G deployment, they should undertake or promote risk assessments to gain fuller visibility into the threat landscape, including the supply chain ecosystem and which risks can be mitigated and which ones cannot. Policies should promote the procurement of equipment from trusted suppliers that adhere to industry-driven, consensus-based international standards, consider geopolitical implications of manufacturing locations, localization and sourcing requirements, and encourage diverse supply chains to help manage risk. Policies should also include a focus on breaking down barriers to trade in technology in order to help with diversification. We recommend that policymakers leverage the Prague Proposals to understand relevant risk assessment criteria and to further effective cybersecurity risk management.

- **Policymakers must focus on threats to the 5G ecosystem beyond those associated with specific supply chain actors and equipment.** While we encourage governments to continue to focus on supply chain risk management, supply chain is only one of the many important 5G risk factors. An exclusive focus on concerns regarding particular suppliers will compromise demonstrative progress towards securing 5G. Instead, policymakers should consider adopting policies that seek to manage the full range of security risks to mobile network infrastructures, applications, and services, including devices and data. For instance, automated and distributed threats such as botnets will likely be a more pervasive issue in the context of 5G network deployment, and policymakers should consider innovative cybersecurity solutions to adequately mitigate such threats, including through the use of AI and other automated tools. Further, a singular focus on equipment alone threatens to stifle what should be strong national attention in all countries on the full breadth of cybersecurity risk factors facing 5G networks.

- **Government and industry must share responsibility and collaborate.** Government and industry share the goals of mitigating cybersecurity threats to network infrastructures, preventing cyberattacks, and reducing the impact of cybercrime. As in all areas of cybersecurity, achieving these goals is a collective effort. Public-private partnerships should be leveraged to ensure that both industry and government arrive at the desired policy outcome of more secure 5G networks. Industry has developed a multitude of security best practices that can be referenced or built upon, and any new best practices should be developed in conjunction with industry. Operational partnerships are key as well, particularly regarding sharing information on threats to 5G. No one organization in the private or public sectors can see all cyberthreats, and industry often does not have access to classified or sensitive government cyberthreat intelligence. It is imperative that both sides work together to fully understand and assess potential threats in order to take appropriate mitigation measures.

4 Standards

Standards for 5G must be industry-led. Competition drives innovation in industry-led standards settings, as competition among contributions to a specific standard improves that standard, and competition among standards allows for optimal market-based choices. Ultimately, the information and communications technology (ICT) industry builds to voluntary, global, industry-led consensus-based standards that are accepted or chosen by the marketplace as the most effective or most appropriate. This is no different for 5G. Government policymakers can play an important role by supporting and promoting this industry-led standards development process, participating in it where appropriate, and by working to ensure that their country's policies point to and leverage global standards.

- ✔ **Policymakers should support globally harmonized 5G standards or technical specifications.** Governments should avoid promoting or mandating country-specific standards that could lead to a balkanized system resulting in varying national requirements, jeopardizing interoperability of products as well as security and reducing the value of mobile connectivity for citizens. This means that governments also should support their industries' – and all companies' – full participation in international standards development bodies. A harmonized international system depends on the contributions and participation of all relevant stakeholders, including governments, to develop standards that are most appropriate for the market and current technology.

- ✔ **Governments should uphold and promote best practices in all fora where standards and specifications are being developed.** International standards provide technical specifications that enable products to operate across markets, meet consumer needs, support implementation of strong security measures, and drive economic opportunity for every sector of the economy. Governments and the private sector alike must protect and promote international standards and the rules-based processes that enable consensus-based, industry-driven development of technical standards. Standards and specification development processes have built-in rules and safeguards that prevent any actor from single-handedly producing a standard. These rules and processes also support transparency of technical elements that is essential for trust of any system. As a means to protect and promote this rules-based system, governments should avoid taking a top-down approach and should encourage consistent industry engagement, without directing or controlling industry's activities.

- ✔ **Policymakers should encourage consistent industry engagement in international standards activities while also engaging where appropriate.** Consistent engagement in international standards development organizations is crucial to understanding the system, developing influence, and effectively competing and cooperating with other companies and stakeholders to harmonize technical standards for the benefits of citizens and industry alike. It is also essential to the value of transparent processes that technical specifications are being reviewed by qualified experts. Governments should also consistently engage in international standards development activities as appropriate.

ITI's 5G Essentials for Global Policymakers

ITI's 5G Essentials for Global Policymakers provides a helpful and necessary context on the issues ITI and its member companies believe to be of importance to those seeking to better understand the recommendations set forth in our 5G Policy Principles.

As the premier technology trade association with a presence across the globe, ITI represents the full spectrum of technology companies, including those contributing to nearly every facet of 5G, from the equipment at the core to the applications that will run on top of 5G networks.

1 What is 5G?

Simply put, 5G is the next generation of network technology. 5G can utilize existing 4G network infrastructure in some cases, although it is an enormous shift away from legacy telecommunications systems to an information technology-based infrastructure. 5G will bring new equipment and software, and spectrum – such as small cells, software-defined networks, and very high frequency spectrum. Although 5G can build off of existing infrastructure, it is not only an incremental improvement over previous network technology. While 5G deployment is in the early stages, it is already being deployed in public and private settings.

Some of the key commonly understood features that characterize 5G are:

- **Massive connectivity:** Radio Access Network (RAN) will be able to support 100x more connected devices. 4G networks support approximately ten thousand devices per square mile, while 5G should support about 100x this number = one million devices per square mile.
- **Ultra low-latency:** The amount of time it takes for data to be transmitted from its source to the destination point on the network is less than 1 millisecond, which is 400 times faster than the blink of an eye. Low latency results in 5G being significantly faster than 4G and is important for time sensitive applications and services such as high-definition streaming video, smart vehicles, precision manufacturing, and critical services and infrastructure control.
- **Extreme mobility:** 5G will allow the ability to maintain connection without interruption or loss of quality while moving at high rates of speed.
- **Increased capacity:** By utilizing higher spectrum frequency, 5G will be able to carry more data. It is expected to support 100 times the amount of data traffic as compared to 4G.

5G by the Numbers

5G will have a tremendous economic impact and effect on data. The implications of these numbers are significant not only because 5G will power the next wave of data-driven innovations, but also because of implications for individual privacy, national security, technological leadership, and economic competitiveness.

Economic Impact:

$13.2 T — Globally, 5G technology is expected to enable $13.2 trillion in economic output by 2035.[4]

$275 B — In the United States alone, 5G is expected to generate up to $275 billion in infrastructure investment, thus creating approximately three million new jobs and boosting GDP by $500 billion annually.[5]

Data:

38 EB /month in 2019 to **160 EB** /month in 2025 — 5G networks will enable increased speeds and staggering amounts of data – mobile traffic is expected to grow by a factor of 4 from 38 exabytes in 2019 to 160 exabytes per month in 2025 (exabyte = one billion gigabytes).[6]

[4] https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study-2019.pdf
[5] https://www.accenture.com/_acnmedia/pdf-82/accenture-strategy-accelerating-future-economic-value-2018-pov.pdf
[6] https://www.ericsson.com/en/mobility-report/reports/november-2019/mobile-data-traffic-outlook

2 The Importance of Spectrum to Deployment

Spectrum is the collection of airwaves that wireless signals travel over, the invisible medium that connects with the broader network. The amount of spectrum available is perhaps the most important factor that determines how much bandwidth or throughput 5G systems can support. Licensed, unlicensed, and shared licensed spectrum play important roles in enabling the full value of the 5G innovation platform.

- **Licensed spectrum** is where a user pays a fee for the exclusive right to operate on an assigned frequency. Spectrum rights are managed by governments, often a designated regulatory agency with information and communications technology (ICT) expertise
- **Unlicensed spectrum** is swaths of the airwaves where any user can transmit under certain power limits.
- **Shared spectrum** allows multiple categories of users to safely use the same frequency bands. Often this takes the form of tiered users, where certain users have primary access and other users can operate so long as they did not cause interference. Sharing may also take place on a temporal or geographic basis.

The current generation of fixed and mobile networks relies primarily on the lower range of radio frequencies under 3 GHz, referred to as low-band spectrum. For the first time ever, we are seeing a type of network technology that can operate over a much broader range of radio frequencies to include high-bands. Spectrum in low-, mid-, and high-bands is needed for 5G, though there has been specific focus globally on making more high- and mid-band spectrum available.

- **Low-band** (e.g. < ~1 GHz) spectrum, due to its propagation characteristics, is able to travel farther so carriers use this spectrum to cover larger geographical areas without signal interruption.
- **Mid-band** (e.g. 3.5 GHz) is considered the "sweet spot" of spectrum, offering a combination of both coverage and capacity.
- **High-band** (e.g. mmWave) spectrum offers wider bandwidth, which carries more data faster, providing higher data rates. Signals do not travel as far as lower spectrum, so 5G deployment in these bands is using a denser network of small cells operating at lower power than traditional macro cells.

3 How Standards Enable 5G Development and Rollout

Standards are essential to 5G deployment in that they facilitate interoperability of devices and solutions. For example, the fundamental promise of 5G for mobile applications is that any mobile device can speak to any other mobile device over any network, which will help to realize the economic benefits of 5G. In addition to interoperability, cybersecurity of 5G networks is also supported by industry-developed standards and guidelines. Those 5G specifications and guidelines are being driven and developed by a variety of standards development organizations with participation from thousands of experts from industry, government, academia, and research organizations.

Given the breadth and complexity of the work, it is important that companies are able to choose the most appropriate body in which to participate to advance their work. There are a wide variety of standards development organizations and consortia, each with their own procedures to develop standards and specifications. Market forces enable companies to coalesce around the "right" standards bodies for the right work. An illustrative, but by no means exhaustive, list of bodies engaged in 5G standards, guidelines, and specifications development is below:

- **3GPP:** By and large, the focal point of development for 5G specifications and standards is the Third Generation Partnership Project (3GPP), a consortium made up of seven of the regional telecommunications standards development bodies. 3GPP has hundreds of technical specifications under development for mobile wireless communications, including the air interface/radio access (5G New Radio), the 5G core, and the IoT, among others. 3GPP is also developing standards for networks to interconnect collaborate with one another. For example, 3GPP's non-public network support is intended to allow private networks optimized for a specific purpose (e.g., an automated manufacturing facility) to co-exist with public carrier networks.
- **GSMA:** GSMA is an industry association representing the interests of mobile operators worldwide, including more than 750 operators and almost 400 companies in the broader mobile ecosystem. GSMA has published hundreds of security guidelines, recommendations and requirements over the years regarding best practices in mobile security that support real-world deployments related to security of devices, networks, interconnect protocols, and services. GSMA's Fraud and Security Group is particularly active, working on 5G security in the context of other interdependent topics such as IoT and roaming.
- **International Telecommunications Union (ITU):** The ITU is in the process of developing ITU-R Recommendations for the terrestrial components of the IMT-2020 radio interface(s) based upon specifications from external, industry-led standards developments organizations.
- **O-RAN Alliance:** The O-RAN Alliance is working to build specifications and standards for 5G networks, focused on open and interoperable interfaces for radio access networks.
- **Internet Engineering Taskforce (IETF):** IETF covers specifications related to 5G non-radio network segments.
- **Institute for Electrical and Electronics Engineers (IEEE):** IEEE is involved in the creation of many standards, including WiFi and WiMAX standards, as well as other machine communications standards that will change with 5G.

4 Emerging ICT Technologies

There are a host of other technologies that are helping to drive the development and deployment of 5G networks, including network slicing and virtualization. Below are some key technologies explained:

- **Massive MIMO (Multiple Input/Multiple Output):** A wireless technology that uses multiple transmitters and receivers in a minimum 16X16 array to transfer multiple data signals over the same radio channel. This results in higher capacity, greater spectral efficiency, and faster speeds.
- **Network Slicing:** Unlike some earlier wireless technologies, 5G networks have sufficient capacity such that they can be segregated into individual channels utilizing the same physical infrastructure. This so-called "slicing" allows operators to optimize the network for different use-cases, making networks more agile, flexible, and able to address different customer needs.
- **Network Functions Virtualization (NFV):** Virtualization separates the network functions from hardware on a network and allows them to be managed through virtual machines, including through cloud-based solutions. This presents an opportunity for software applications to be run on widely available hardware, allowing 5G networks more flexibility than previous generations.
- **Software Defined Networking (SDN):** In previous generations of network technology, routers and switches controlled and forwarded data transmissions on the network. SDN separates the control function from the forwarding function, with a greater emphasis on consolidating this control function into a single network controller that can communicate and direct the entire network. Similar to virtualization, SDN offers significantly more flexibility and facilitates automation in the network.
- **Spectrum-Sharing:** Modern systems for avoiding harmful interference among co-users are freeing up new spectrum bands for 5G uses (e.g. the Citizens Broadband Radio Service in the U.S. and shared spectrum bands in the UK and Germany). This approach is especially useful when existing spectrum bands have incumbent users that are difficult to relocate.
- **Edge Computing:** Edge computing moves the data compute, storage, and processing functions closer to the IoT endpoint and/or end-user, which improves efficiency of processing and latency. 5G will harness edge computing in a way that previous generations of network technology did not, helping to meet performance requirements.

5 The Importance of Security in 5G

Security is fundamental to successfully deploying and using 5G. The future will be filled with exciting new applications and services that will run on top of 5G, but an increasingly connected world will also increase security risks, ranging from an accelerating and evolving cybersecurity threat landscape to concerns regarding sophisticated adversaries exploiting supply chain vulnerabilities. Given this increased interconnectedness, emerging threats can pose a danger to the 5G ecosystem more widely if not adequately planned for and managed. The good news is that 5G networks and standards are being designed with security in mind from the outset, and 5G networks will include several security enhancements that will enable business and government enterprises to confidently deploy new applications and IoT services to harness the full value of 5G. While investments in 5G infrastructure and the accompanying digital transformation are well under way, consumers, businesses, and governments should prioritize security during the transition and seek to leverage the security enhancements available for the first time in 5G.

Industry around the world is actively working to secure mobile networks, including 5G. This includes investing time and resources into developing cybersecurity technologies and services to secure 5G networks and the applications and services running over them, helping to educate business leaders on the importance of cybersecurity investments, sharing operational threat information on threats traversing mobile networks so that relevant parties can take action, and participating in the development of relevant global 5G security standards and reference documents. Industry and government are also collaborating via public-private partnerships to ensure that we arrive at the desired policy outcome of more secure 5G networks, including operational partnerships to share information on threats to 5G, and partnerships to further supply chain risk management best practices and solutions. No one organization in the private or public sectors can see all supply chain or cyber security threats so it is imperative that both sides work together to fully understand and assess the full range of potential security threats in order to develop and implement appropriate mitigations.

6 5G Will Power Data Driven Innovations

The increased speed, capacity, and functionality of 5G networks will help to enable the next generation of data-enabled innovations such as the internet of things (IoT) and artificial intelligence (AI).

6 5G Will Power Data Driven Innovations *(continued)*

Specific Use Cases Envisioned for 5G:

Agriculture

5G can enable new precision agriculture capabilities, allowing farm equipment to stream data back and forth in real-time. Specific examples of this include: leveraging sensors to communicate soil nutrition levels and report on current and predicted weather patterns; allowing for improved crop management and livestock analysis; directing autonomous vehicles to perform field tasks, such as harvesting; and bringing in-field expert advice to communicate with individuals working in remote farming areas.

Manufacturing

Currently, manufacturers rely primarily on fixed-line networks to support critical applications, but 5G could allow for lower costs, higher flexibility, and low latency performance for factory floor productions and alterations. By combining the data generated from 5G-connected sensors with machine learning algorithms, companies could monitor equipment in real-time and predict with greater accuracy which machines are about to fail, reducing the likelihood of costly downtime.

Healthcare

5G can help expand the possibilities for telemedicine as well as applications in hospital settings, allowing patients to be treated sooner and access a broader range of specialists. The availability of remote patient monitoring can improve health care delivery and enhance preventative care. The increased bandwidth of 5G can transport large data files like medical imagery and 5G's lower latency allows real-time high-quality video, enabling the use of augmented reality (AR) and virtual reality (VR) in surgical procedures.

Retail

From small grocery stores to large hotel chains, retailers of all sizes could leverage 5G technology to improve their operational efficiency. For example, by using IoT-embedded sensors, a store would have a real-time view of its stock and could seamlessly communicate to the supply chain to send a new shipment when a particular product is low. 5G will also enable retailers to use technologies such as personalized digital signage, interactive mobile apps, and virtual reality to both ease and enhance the overall customer experience.

6 5G Will Power Data Driven Innovations *(continued)*

Specific Use Cases Envisioned for 5G ***(continued):***

Smart Cities and Communities

The deployment of smart cities is reliant on the connection of multiple low-power digital devices to help power homes, offices, and communities through the IoT. Due to the high volume of data that must be collected and maintained to support this level of real-time connectivity, smart cities need the higher speed and larger capacity offered by 5G. Examples of smart city use cases include: smart traffic management and public transit systems (e.g., reducing rider wait time and optimizing bus inventory), smart grids and energy systems (e.g., enhancing demand-side management to help reduce electricity peaks and reduce costs), smart outdoor lighting (e.g., automatically dimming public lighting when no vehicles or pedestrians are present), and smart homes (e.g., controlling indoor lighting, entertainment systems, and appliances).

Public Safety

5G can help optimize public safety by allowing real-time access to mission critical information, improving connectivity, and ensuring reliable communication. 5G specifications will ensure that communications to or between first responders are prioritized in times of emergency, will help to provide first responders a high degree of situational awareness, and will ultimately lead to improved safety of responders and better outcomes all around.

Education

5G in education, particularly in underserved areas, can dramatically change the nature of education through enhanced learning technologies, including the use of AR/VR tools, which rely on 5G, resulting in closing persistent achievement gaps.

7 Common Misperceptions About 5G, Explained

MYTH: 5G is less secure than other generations of network technology.

FACT: 5G considers security at the outset, instead of as an afterthought. As a result, 5G has the potential to be more secure than previous generations of network technology. While the increased reliance by a wide swath of industries and critical infrastructure providers on 5G, coupled with the proliferation of connected devices enabled by 5G will result in more entry points into the network and the potential for increased cybersecurity challenges, the numerous security enhancements built in to 5G networks will help secure communications as well as the IoT and other innovations 5G helps enable.

Standards development bodies are working on 5G security standards. For example, 5G specifications will ensure that data integrity is achieved at every layer of the network, improved authentication measures are employed, and privacy enhancements are introduced. New industry reference documents are guiding operators on how to automatically detect and block threats and mitigate security risks. It will be imperative for operators to leverage standards and best practices, invest in state-of-the-art security technologies, and keep current on network security updates and good cyber hygiene. In addition, 5G will benefit from many technology evolutions already used in other industries, such as virtualization and micro-segmentation that are being deployed in large enterprise data centers and public cloud providers. 5G has the opportunity to benefit from the knowledge gained in the security developments in these adjacent markets.

MYTH: 5G is only about increasing download speeds.

FACT: 5G is about much more than just increasing download speeds – it is also about greater connectivity, lower latency, capacity, and network performance, all of which will usher in a new era of devices, applications, and services available to consumers and businesses alike. For example, we expect to see 5G-enabled applications across numerous sectors, including in manufacturing, agriculture, healthcare, and transportation. This will generate tremendous economic impact. Consumers will see improved video streaming, greater home automation, and new applications around augmented reality. Because an exponential amount of data will be sent between all parties at much faster speeds, appropriate spectrum must be quickly and efficiently allocated and security must be built in from the beginning.

MYTH: 5G standards are nearly finished.

FACT: 5G standards, as with most other technical standards, are and will remain under continuous development in 3GPP and a number of other standards bodies including O-RAN Alliance, IEEE, IETF, ISO, ITU and ETSI, and these standards will continue to change as the technology evolves. For example, 3GPP issues technical specifications in "Releases," whereby a core set of features are "frozen" and subsequent functionality can be added on in future Releases. It is important to note that 3GPP technical specifications are backwards and forwards compatible, ensuring that a system can continue to perform without interruption as network technology evolves.

7 Common Misperceptions About 5G, Explained *(continued)*

MYTH: China is taking over 3GPP and other standards development bodies and will therefore wield undue influence in the deployment of 5G networks.

FACT: As 5G is deployed and 3GPP continues to develop the technical specifications that will govern this next generation of network technology, some have raised concerns that China is "flooding" the system, putting forward large numbers of contributions and sending increased numbers of participants to meetings. However, the quantity of contributions is not an accurate way to measure or predict influence; what really matters is the quality and substance of a technical contribution and which ones are accepted for inclusion in the specifications. Additionally, few contributions put forth by one company go through the process without modification. 3GPP is a consensus-based, collaborative organization, with rules and processes in place to ensure that no company or country has undue influence or is able to micromanage an agenda. There is no empirical evidence of undue influence by any actor on 5G standards both in the distribution of leadership positions and in accepted contributions of leading 5G specifications. Firms participating in 3GPP do have influence based on the technical merit of their contributions, but there is no evidence that Chinese firms have disproportionate, meaningful influence at 3GPP or other SDOs.

MYTH: Only U.S.-based manufacturers produce safe/secure equipment.

FACT: Equipment security is not solely determined by country of origin. Security is a continuum, not an end state. While country-of-origin is one risk factor to be considered, it is not the sole and dispositive factor. For instance, the U.S. Department of Homeland Security ICT Supply Chain Task Force recently undertook a supplier threat assessment and country-of-origin was identified as one threat out of over one hundred potential factors to take into consideration.

MYTH: The primary security risk in 5G networks is associated with hardware.

FACT: While hardware is certainly one area that could present a risk in the network, security solutions will need to focus on all aspects of the end-to-end system.

Cyberattacks on mobile network infrastructure (3G, 4G, and now 5G) and their users continue to grow, along with increased network capacity and speed. Criminals consistently introduce and update new attack tools, using automation and exploit toolkits, to attack mobile operators' network infrastructure, applications, and services, and the operators' customers/end-users (consumers and enterprises). As 5G will support an increased amount of connected devices, the attack surface also increases. The risk and potential damage are relevant not only to the telecom sector, but to all sectors to which it is closely interconnected and interdependent including energy, finance, healthcare, transportation, IT, government, manufacturing, and retail. That said, governments should consider risks beyond those associated with hardware.

7 Common Misperceptions About 5G, Explained *(continued)*

MYTH: There is no need for an edge if your radio access network is connected by fiber to the core.

FACT: The 5G network design has been specifically architected to flatten the hierarchical design of previous generations of mobile network and push compute, storage and connectivity as close as possible to the service delivery point, also known as the edge of the network. It is the network edge where use cases that involve the need for ultra-reliable low-latency are enabled. The close proximity of the edge to the running service, for example, Robotic Surgery, creates the low latency capability between the Robot (UE) and the Service that is attached to the Robot. Thus, an edge is a vital part of the 5G network.