June 2020

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**
2. **Enabling 5G Deployment and Access to Spectrum**
3. **Security**
4. **Standards**

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.