US Ignite Comments on NTIA National Strategy to Secure 5G Implementation Plan

On behalf of US Ignite, thank you to the National Telecommunications and Information Administration (NTIA) for the opportunity to submit the following comments in response to Docket Number 200521-0144 *regarding a National Strategy to Secure 5G Implementation Plan.* A National Strategy to Secure 5G will better protect companies and institutions, ultimately strengthening U.S. economic prosperity and national security. In this spirit, the comments below reflect US Ignite's recommendations on actions the federal government must take to ensure the security of future 5G networks.

About US Ignite:

US Ignite, a nonprofit organization dedicated to advancing the "smart community" movement in the US, is a catalyst for innovation in smart community services that are powered by a new generation of advanced wireless technologies. With ongoing partnerships with the National Science Foundation (NSF), the National Institute for Standards and Technology (NIST), and the Department of Defense, US Ignite's work in the deployment of advanced wireless technologies as a testbed facilitator and trusted partner in smart community development is unparalleled. For instance, US Ignite, in partnership with Northeastern University, manages the $100 million NSF-funded Platforms for Advanced Wireless Research (PAWR) program as the leader of its project office. This program has created testbeds and pilot programs in Salt Lake City, New York, and Raleigh for the deployment of new technology while also enabling researchers to conduct advanced research without having to spend capital to develop new R&D infrastructure.

US Ignite's Comments

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 current public health crisis we are facing due to the COVID-19 pandemic demonstrates why is it is critical to ensure that 5G wireless infrastructure is developed domestically and in a secure fashion so that Americans are not denied access in a future emergency. A few key lessons can be taken from the recent public health crisis:

a) Broadband networks, including not just core facilities but last-mile connections to residences and businesses, are critical infrastructure that allow millions of Americans to continue accessing education, working and remaining productive; and
b) Securing and hardening this critical networking infrastructure, including the supply chain that manufactures its parts and equipment and the software that makes it run, is a matter of vital national importance.

c) The dramatic increase and escalation of cyberattacks against a variety of organizations demonstrates that in developing a 5G architecture, **security should not be considered after the fact**. US Ignite recommends the federal government, in particular the Department of Defense (DOD) and the Department of Homeland Security (DHS), should co-lead establishing the necessary security standards & requirements for domestic and overseas operations to ensure National Security. The requirements will need to drive the necessary supply chains to ensure the domestic supply of RF components, integrated chips sets, devices and services are secure. A national security-based network that embraces a provider neutral/open standards architecture to ensure security, promote innovation and competition, is inherent to the roll out.
d) A workforce is needed to carry out any federal investments in 5G, and to ensure that future technologies and architectures are effectively adopted and deployed throughout the country. The federal government should consider dedicated workforce programs ranging from certificates to PhDs to ensure the future workforce can step up and address the science and technology challenges the US will face now and in the future

One key aspect of addressing the challenges facing the US today is to ensure that there are open, secure, and reliable sources of 5G equipment and software available to US network operators regardless of geopolitical concerns or disruptions to the global supply chain. While current mobile carrier networks are built to international standards (e.g., 3G or 4G), the software that runs the equipment in those networks is proprietary and is owned by chip and radio manufacturers. This makes innovation more difficult, as any company trying to innovate to provide lower cost or improved equipment often must either pay to use software from others or create its own network software from scratch – a lengthy and expensive proposition. It is critical that the architecture for 5G networks be open and interoperable so that future advanced networks are not dependent on one equipment manufacturer, especially not one operating or beholden to an adversarial nation. To accomplish this, US Ignite offers the following recommendations in response to NTIA's questions below.

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

To achieve the technology goals and outcomes discussed above, the federal government should invest additional funding into research and development (R&D) to develop Open Radio Access Network (open RAN) technology. US Ignite recommends that NTIA establish a **Wireless Supply Chain Innovation Grant Program,** as proposed by the House and the Senate in the *USA Telecommunications Act*. As proposed in the bill, NTIA would establish a $750 million grant program that would see to achieve the following:

a) Promote the development of technology, including software, hardware, and microprocessing technology, that will enhance competitiveness in the fifth-generation (commonly known as "5G") and successor wireless technology supply chains.
b) Accelerate development and deployment of open interface standards-based compatible, interoperable equipment, such as 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.
c) Promote compatibility of new 5G equipment with future open standards-based, interoperable equipment.
d) Manage integration of multi-vendor network environments.

e) Create objective criteria to define equipment as compliant with open standards for multi-vendor network equipment interoperability.
f) Promote development and inclusion of security features enhancing the integrity and availability of equipment in multi-vendor networks.
g) Promote the application of network function virtualization to facilitate multi-vendor interoperability and a more diverse vendor market."

US Ignite proposes to bring its multi-stakeholder consortium model to bear in assisting NTIA with these efforts. This model, developed as a part of US Ignite's $100 million PAWR program, would allow NTIA to maintain a focused, long-term partnership with a variety of federal, academic, and industry stakeholders. It could be used to establish and support an R&D consortium to host and maintain open RAN technical contributions under an open source license and to provide incentives for code contributions, proofs of concepts, and joint technology development, and it could better achieve the long-term goals of this program than would be available by funding small, disparate research efforts. US Ignite also recommends that NTIA learn from and leverage the NSF-led PAWR program that has stood up open access wireless research testbeds at locations across the country.

3) 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.

US Ignite believes that federal investment in research and development is critical to advancing open RAN research and establishing a secure 5G architecture. Ultimately, this requires a whole of government approach that brings in international partners and allies to collaborate on R&D and engineering to achieve our 5G goals. US Ignite recommends that, in addition the proposed Wireless Supply Chain Innovation Grant program described above, the federal government should undertake the following R&D efforts:

a) Focus investments towards system security and resiliency on an engineering and strategic level.
b) As noted above, invest in STEM education and workforce programs, ranging from certificates to PhDs, to develop a workforce that is capable of researching, developing, and deploying 5G and next generation wireless technologies and network architectures.
c) Encourage investment in the Internet-of-Things and Industrial-Internet-of-Things -- Massive deployments of IoT nodes need well-tested end-to-end system deployments and holistic research and innovation contributions not only across all layers of protocol stack but even from an architectural perspective as we proceed towards virtual network slices. The federal government should be actively pushing for employing open-source initiatives like ONAP and open RAN in the IoT sector.
d) Preventing the network infrastructure of military bases from cyber-attacks through hardened, vetted solutions from open approach of 5G deployments by promoting and funding research focused across different bands of spectrum, beyond just mmWave spectrum. Additional information on this topic can be found at https://spectrum.ieee.org/tech-talk/telecom/standards/how-america-can-prepare-to-live-in-chinas-5g-world.

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

US Ignite recommends that the following actions could help bring further investment in R&D from the commercial ecosystem:

a) Issue prize challenges that bring government, industry and academia together as teams to solve challenges, including high profile competitions to better utilize network resources to achieve the goals of high spectral efficiency and co-existence (similar to the DARPA Spectrum Challenge).
b) Create regional science and engineering consortiums that focus on 5G development and meet the needs of unique geographic, economics challenges of that region.
c) Empower the National Institute of Standards and Technology (NIST) to serve as a clearing house for commercial technologies that can be introduced into future network ecosystems.
d) Provide incentives for using domestic hardware, including special research grants for academic and industrial research labs who commit to demonstrating outcomes on domestically-produced hardware.
e) Solve problems related to both rural network deployments as well as ultra-dense urban network deployments. While the former poses unique challenges for sparse settings, the latter calls for solutions for problems related to highly populated areas. Solutions for other demographic distributions can be obtained by interpolating the above two deployment cases.
f) Encourage collaborations with wireless carriers and equipment manufacturers to foster R&D efforts with academia, including the funding of joint academic-government-industry research fellowships to attract research talent.