Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

KEYSIGHT TECHNOLOGIES

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

June 18, 2020

Re: Keysight Technologies Comment in Response to NTIA request for public comment on Implementation Plan for National Strategy to Secure 5G; RIN #0660-XC04

Dear Mr. Hall,

Keysight Technologies appreciates the opportunity to submit our response to NTIA's request for comment, on behalf of the Executive Branch, on developing an Implementation Plan for the National Strategy to Secure 5G (hereafter the "5G Strategy Plan").

Keysight Technologies is the world's leading electronic test and measurement company with our roots as the legacy Hewlett Packard company. We enable innovation worldwide especially in 5G and beyond. We provide solutions and innovations in every layer of the 5G stack, enabling 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 U.S. Government's increased focus on deploying the next generation of network technology; indeed, 5G will be transformative and offer opportunities to U.S. companies that were not previously available. We further appreciate the comprehensive nature of the National Strategy to Secure 5G – all four lines of effort are imperative to ensuring U.S. leadership in this space. We have commented on all four lines of effort below for your consideration.

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)?*

First and foremost, the Federal Government should promote and support U.S. companies in the 5G commercial ecosystem to include test and measurement

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

vendors who enable 5G and beyond.

The basis for sound 5G policy rests on ensuring an environment that supports innovation and encourages the investment in foundational and new technologies that facilitate the next generation of networks, while also driving deployment by freeing up more spectrum and taking steps to make 5G deployments easier and ensuring that there is continuous and thorough testing throughout the 5G ecosystem from beginning to end of the workflow.

- Continuous 5G Testing up front and early from Design, Validation, Quality of Service, Standards Conformance, and Security
- Prioritize freeing up additional spectrum for 5G and beyond.
- Invest in the 5G workforce - from tower technicians and telecom crews servicing 5G infrastructure to datacenter technicians, cloud systems administrators, cybersecurity experts, radio and signal processing engineers, communications systems engineers, and other workers with the skills to advance 5G.
- Streamline siting requirements to speed up the deployment of 5G infrastructure
- Additionally, DoD should establish a 5G working group and this 5G working group should include participation by U.S. based 5G industry enablers from test and measurement to handset manufacturers.

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

The U.S. Government can promote and foster the research, development, testing, and evaluation of new technologies and architectures through the following:

- Ensuring that testing and evaluation is a priority, upfront and early and not an afterthought. It needs to be part of the initial discussion of any new 5G technology or testbed/network.
- Fostering opportunities for public-private partnerships, government sponsored initiatives, cooperative agreements, and grants to support ongoing research and development.

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

- 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.

- Supporting 5G/5G+ standard organizations and the development of open and transparent standards to drive consistent evaluation of 5G systems. This would go above standards just related to technical performance, but include quality of service, quality of experience, security standards, and others.

- Increasing access to and outreach by 5G government leaders to industry and incentivizing the sharing of 5G innovations and technologies.

- Supporting R&D tax credits around 5G research and development by U.S. companies and academic institutions.

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?*

The U.S. Government should take the following steps to motivate the domestic-based 5G commercial ecosystem to increase 5G research, development, and Testing:

- Provide incentives for cross-industry collaboration especially between WiFi and personal-area networks (e.g. Bluetooth) and 5G cellular and between 5G cellular and the satellite, UAV, and HAPS industries.

- The U.S. Government should leverage the approach that the EC has used in their Framework Programme's (most recently "Horizon 2020" and "Horizon Europe") that provides significant research funds for large-scale and small-scale public/private/academic consortia projects. The NSF PAWR testbeds represents a small step in this direction but could be expanded.

- Develop a framework for intellectual property management as well as a framework to address issues related to anti-trust statutes.

- Promote open 5G architectures to allow more U.S.-based vendors to participate in the implementation of 5G across the U.S. These open architectures should be tested for compliance to APIs / interfaces / standards by using tools and equipment from U.S.-based test vendors.

- Expanding and leverage existing Other Transaction Authority (OTA) agreements to incentivize private sector investment in 5G by providing seed funding for prototype projects. This arrangement is advantageous for private

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

sector companies as the technical risk is shared between the Government and industry. These 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. Fully tested and accredited technologies can then move more quickly toward wide-spread Government adoption through subsequent procurements. This acts as further incentive for companies to participate in Government-sponsored R&D for emerging technologies like 5G and beyond. Again, testing is key throughout the process and it should be continuous and in-depth.

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.*

The following areas of research and development should be a priority to achieve and maintain U.S. leadership in 5G:

- The U.S. Government should elevate R&D related to virtualized architectures and software-defined networking to more rapidly increase competitiveness in 5G.

- The U.S. Government should prioritize and increase R&D spending for 5G use cases, including those related to RF Coexistence, Autonomous Vehicles, the Internet of Things, Artificial Intelligence, Real-Time End-To-End Testing and Sensing, Real-Time Security monitoring, and network resilience.

- The U.S. Government should elevate R&D related to "beyond 5G" ("Network 2030" or "6G"). This would include advanced next-generation networking protocols, advanced higher-frequency radio systems, advanced security systems, and the application of artificial intelligence to all of these technologies and innovations.

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

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

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

The U.S. Government should consider the following factors in the development of core security principles for 5G infrastructure:

- The U.S. Government should incentivize U.S.-centric standard organizations to develop Cyber/5G security compliance requirements that require certification through independent testing/assessment bodies. This certification process of security standards could be a gold standard requirement used to lead influence global standards bodies to common baseline. i.e. the U.S. Government should strive for a global baseline and have incremental facets to the standard that make the U.S. systems more immune to threats, more aware of threats, and more resilient when threats do make inroads.

- The U.S. Government should sponsor open source based 5G development which will promote transparency and competition and lead to more robust 5G infrastructure, security and services.

- The U.S. Government should develop and require standards and conduct test, measurement and assessments for security and cybersecurity throughout the development, deployment, and operation of 5G networks. Security should be robust and designed in from the beginning. This would include both the inclusion of security protocols within the evolving 5G standards as well as minimum security standards for 5G infrastructure hardware and software. This should involve secure coding practices, white and black-box testing, continuous assessment and monitoring of deployed infrastructure to detect suspicious activity and undue risk.

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?*

The U.S. Government should consider the following when evaluating the trustworthiness or potential security gaps in U.S. 5G infrastructure, including the 5G infrastructure supply chain:

- First and foremost, full transparency is an absolute requirement for trustworthiness.

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

- Testing and measuring security effectiveness from both individual network elements/functions and complete end-2-end infrastructure perspectives.

- Incorporating the relevant 5G security principles recommended by the "Prague 5G Security Conference" - The Prague Proposals.

- Developing a 5G security certification program established through rigorous independent testing/assessment.

- Determine minimum standards for 5G security testing of infrastructure hardware, analogous to the FIPS requirement for computing and networking equipment, should be developed due to the length and complexity of supply chains which presents special challenges to infrastructure security.

- Requiring independent source code and component validation. Additionally, the use of open-source code should be encouraged wherever possible because even an otherwise secure piece of hardware or software may be rendered insecure by the inclusion of a single component or software library.

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?*

The following verifiable and adoptable security control regimes are extremely important to a secure 5G network:

- It should be standards based driven by global standards bodies and enhanced for U.S.-specific national security concerns.

- The standards should be developed by cross-industry consortia so that they are meaningful, useful, practical, verifiable, and can evolve with the state of the art in technology.

- There should be a certification of compliance to the standards by both vendors and independent validation labs.

- There should be a consistent and dependable process to address non-compliance of the standards (e.g. Vendors who supply noncompliant infrastructure hardware or software, or who are found to be noncompliant by independent labs and do not promptly address identified gaps or risks. These vendors should be barred from the 5G supply chain).

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

- There should be a required process for trusted vendors to fully disclose any gaps or risks that they discover in order to inform all affected parties.

- Vendors should follow a Risk Management Framework (RMF) that considers effectiveness, efficiencies, and constraints based on applicable laws, policies, standards, or regulations. For example, NIST SP-800-* publications as specified in the NIST RMF overview "FISMA Implementation Project".

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

There are stakeholder-driven approaches that the U.S. Government should consider in promoting adoption of policies, requirements, guidelines, and procurement strategies necessary to establish secure, effective, and reliable 5G infrastructure, for example:

- Stakeholders should be part of the standards development process ("skin in the game" and source of appropriate subject-matter expertise).

- The standards process cannot operate in a U.S.-centric vacuum. Communications systems are connected globally and to be affordable, need to be based on international standards; hence the standards should have their foundation in those created by global standards development organizations.

- The validation and compliance process should be consistent and transparent.

- Mandating a certification process to a set of testing standards for security and reliability that is required by all suppliers of 5G hardware and software. A certification process is a very useful tool to improve security of the supply chain and 5G ecosystem similar to the UL certification conformance model.

- The implementation of a required 5G certification process by the U.S. government would be instrumental in ensuring that all required standards such as security are met. This would go a long way in trusting the vast number of connected 5G devices.

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*

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

KEYSIGHT TECHNOLOGIES

addressing these gaps? Are there incentive models that have proven successful that could be applied to 5G infrastructure security?

Incentives are important in addressing security gaps in a 5G infrastructure. The types of incentives the U.S. Government should consider are the following:

- Instituting a program like the Bug Bounty Programs that is offered by some of the top U.S. hi-tech firms is a proven model to quickly explore and fix security vulnerabilities and gaps in industry.

- Establishing a 5G security certification program requiring rigorous independent testing and assessment would be prudent in addressing 5G infrastructure security gaps.

- Security comes at a cost, and history has shown that vendors will avoid those costs when possible and if optional. Having established standards for security, the government can leverage tools such as allocation of spectrum to service providers who deploy only compliant hardware and software and only purchase compliant hardware and software for government use.

- The government should publish lists of manufacturers, vendors, and service providers who have been audited for 5G compliance.

- Disincentives need to be used as well, for examples the requirement that deployed hardware and software need to be certified and standards-compliant.

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

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

The deployment of 5G globally presents enormous economic growth opportunity for U.S. companies, particularly as 5G technology is expected to enable $13.2 trillion in economic output by 2035. The increased speed, low latency, increase capacity, and functionality of 5G networks will help to enable the next generation of data-enabled innovations, technologies, and devices such as the internet of things (IoT), Autonomous Vehicles, Smart Manufacturing, VR/AR systems, Remote Healthcare and artificial intelligence (AI).

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

As countries around the world deploy 5G, U.S. companies have started to capitalize on their 5G investments through substantial business growth and new investments. They continue to seize upon these new networks to implement use cases that were previously unachievable. However, it is imperative that we continue to encourage open and interoperable solutions in the deployment of 5G networks to ensure that a variety of vendors can supply different aspects of the 5G network, thus allowing U.S. companies the opportunity to compete worldwide.

Additionally, the opportunities cross multiple parts of the industry from semiconductors to subsystems to full deployment. They include opportunities in applications development and test, sensing and validation of all facets of the 5G ecosystem.

Finally, the deployment of 5G networks worldwide will provide a robust, fast and efficient method for delivering innovative software solutions and services (health/medicine, entertainment, etc.) that have traditionally been dominated by U.S. companies.

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

The U.S. Government can best address the economic and national security risks presented by using 5G worldwide by the following:

- There is no economic risk to the U.S. of a global 5G deployment as long as there is fair and open competition. This global investment is a huge opportunity upon which many U.S.-based companies are already capitalizing. The risk is disallowing U.S.-based companies from participating and competing in this large global business opportunity.

- Increase the use of interoperable, secure and open standards and relying more on software than hardware driven technologies.

- The U.S. Government should 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, relationship with allies, and the U.S. Government's ability to procure 5G technologies.

- The U.S. Government should coordinate with other regional bodies, such as the EU, to develop common standards so that developed security standards

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

can be enforced more broadly. Having a larger market for products which meet U.S. requirements will not only encourage vendors to develop new and secure products but will also help to improve security of 5G networks worldwide. Ideally, U.S. companies can compete successfully for these deployments.

- Incorporating the relevant 5G security principles recommended by the "Prague 5G Security Conference" - The Prague Proposals.

- Taking a leadership role and increasing its expertise in 5G infrastructure security in order to educate other governments and international partners and relevant NGOs about the risks and security requirements for 5G networks and deployments.

- The security risks of 5G are significant but also not unique to the U.S. Hence, the U.S. must continue to participate in global standards development organizations and help establish a more stringent standard where sensible. Additionally, help establish a compliance process along with an ability to evolve these standards as changes to risk emerge.

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

The U.S. Government should best promote 5G vendor diversity and foster market competition by:

- Opening up more unlicensed spectrum to support 5G and beyond.

- Embracing open radio access networks that support open and interoperable solutions for 5G networks. This would allow for interoperability, supplier diversity, competitiveness, and innovation on a massive scale. Leveraging open and interoperable solutions can help to avoid vendor lock-in.

- Adopting policies that promote the use of open-source development, open API support, and open 5G architectures. For example, encouraging Congress to pass the Utilizing Strategic Telecommunications Act which would create an O-RAN R&D fund to help spur innovation in open, software-based wireless technologies, an area where the United States could be very competitive.

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

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?*

The following incentives could close or narrow 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:

- By having U.S. Government sponsored initiatives that focus on secure developments, deployments and operations of Industrial IoTs, Smart IoTs for municipals, and AR/VR for services that leverage the power of 5G/5G+.
- Tax credits for 5G/5G+ R&D and 5G work force development.
- Include our responses to questions posed under Lines of Effort 1 and 2, which we believe adds to 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?*

The U.S. Government can best lead the international development and deployment of 5G technologies and promote the availability of secure and reliable equipment and services in the market by:

- Passing the U.S.A Telecommunications Act that would create a $500 million Multilateral Telecommunications Security Fund. This fund would provide additional direct support to the United States in its engagements with foreign partners.
- Reconsidering the content rules that currently govern Export Import Bank transactions as they are not necessarily applicable to the tech sector. 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 where IP and R&D may be U.S.-based even if the product is manufactured elsewhere. This aspect is not considered in the current iteration of U.S. content requirements that dictate if Ex-Im can support an

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

overseas deal, thus making it significantly more difficult for Ex-Im to support deals related to 5G technologies.

- Continuing advocacy and engagement on 5G issues through bilateral and multilateral dialogue and engaging with other international partners wherever possible.

- Advocating for secure and continuous real-time testing and monitoring, of 5G networks worldwide especially in countries where cost is a significant driver.

- Working closely with U.S.-based test, measurement, and security vendors to develop and standardize real-time security and testing practices and procedures.

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

Keysight Technologies is leading standards bodies in 5G Test. We do so to ensure testing is done well, securely, and in a transparent fashion. However, a coordinated effort by U.S. companies would go a long way in providing standards inputs that are beneficial to the U.S. and international partners. Standards are an incredibly important driver for 5G technologies. Below are specific recommendations that the U.S. government can undertake to incentivize and support U.S. industry participation:

- Support industry-led bodies with rules-based processes in place. Companies that seek to compete in 5G technologies must participate in international standards development processes, and they must be allowed to choose which bodies are best suited for their specific work.

- Make the United States a more attractive meeting location for standards development organizations to host meetings. Attending standards meetings typically requires a significant amount of travel and time commitment, making the U.S. a more appealing meeting location for those based in the U.S. The U.S. Government can encourage this by facilitating visa applications for foreign standards experts who routinely attend these meetings.

- 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 inadvertently created a situation

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

in which U.S. companies were precluded from participating in technology-related standards development bodies in which Huawei or other listed entities were also a participant.

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?*

The following approaches and tools could be used to mitigate risk from other countries' 5G infrastructure:

- More robust testing and validation of hardware and software solutions by setting up independent testing labs to test and validate hardware and software before they can be integrated into the 5G network/ecosystem.
- Instituting a robust certification process to validate trusted vendors.
- Engagements with international partners to better understand their approach to mitigating risk, and factor this into the U.S. Government's own risk-based tools.
- Continue to collaborate and cooperate with international partners to address identified risks.
- Examining the United Kingdom's approach to risk analysis through their establishment of the Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board—this oversight could be expanded for multiple higher-risk suppliers and could entail establishing criteria for how a supplier is deemed high enough risk for an oversight board.

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 U.S. Government could foster and encourage international cooperation around secure and trusted 5G infrastructure deployment by continued support of industry-led standards organizations that are developing many of the technical specifications, including those related to testing and security.

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

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?*

Recommend that the U.S. government consider a similar approach that the EU has taken in developing the EU 5G Security Toolbox.

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

The U.S. Government could take the following action to fulfill the policy goals outlined in the Act and Strategy by a coordinated, whole-of-government approach to supporting the secure 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 and working in different directions. The appointment of a "5G Czar" in charge of coordinating all ongoing efforts related to 5G would be an excellent start.

Line of Effort 5: Other Comments

The following provides additional comments that did not fit in Lines 1-4 but are critical to the continued success and security of deployed and operational 5G and beyond networks in the U.S. and international partners.

- Establish a group of U.S.-based test and measurement experts with U.S.-based test equipment to ensure all 5G networks are conforming to all standards and security protocols along with the expected quality of service. Ideally, this should be done in real-time and continuous.

- Fundamental to a trusted, secure, reliable and standard conforming 5G network is Testing at all levels of the stack, from design to deployment and done in real-time. This is critical and should not be overlooked or an afterthought. This is fundamental to a successful 5G strategy for deployed and future networks that go beyond 5G.

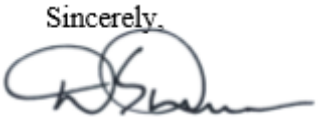
Once again, Keysight Technologies appreciates the opportunity to submit comments and hope that they will be helpful in guiding the White House as it seeks to develop an Implementation Plan for the National Strategy to Secure 5G.

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

800 829 4444T
800 829 4433 F
www.keysight.com

Additionally, we would be happy to further discuss in detail the importance of 5G security and real-time testing and sensing at your earliest convenience.

Sincerely,



Dan Dunn
Vice President ADGS
707 577 2097 T
dan_dunn@keysight.com