June 25, 2020

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, D.C. 20230

RE: The National Strategy to Secure 5G Implementation Plan
[FR Doc. 2020-11398]

Dear Mr. Travis Hall:

IBM appreciates the opportunity to respond to the request for comments on *The National Strategy to Secure 5G Implementation Plan [FR Doc. 2020-11398].* IBM is helping its customers build the next generation of 5G mobile broadband technology networks and is eager to work with NTIA to help the United States develop and deploy competitive, innovative, and secure 5G infrastructure.

We offer three key recommendations for the U.S. government. First, it should promote the widespread adoption of open standards to capitalize on the strength of the U.S. software development and computing industries and ensure that small and large U.S. firms can be domestically and globally competitive in 5G. Second, it should support a robust R&D portfolio for open 5G technologies, both domestically and in concert with trusted international partners. And third, it should develop guidance built around international standards and best practices for cybersecurity, including the Prague Principles and research from the National Cybersecurity Center of Excellence at NIST, while avoiding additional burdensome, prescriptive rules.

Line of Effort One: 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 best way for the U.S. Government to accomplish this would be to promote the widespread adoption of open standards. This would both capitalize on the strength of the U.S. software development and computing industries and ensure that small and large U.S. firms can be domestically and globally competitive.

Unfortunately, some telecom market leaders rely on and continue to build closed 5G technologies that prevent the integration of hardware or software from different vendors. This has created a global chokepoint in the availability of critical 5G technologies.

Closed systems in telecommunications can:

- Dramatically impede competition and innovation. Inhibiting third parties from developing offerings that will work with those systems prevents a "plug and play" approach to 5G, and this lack of competitive pressure reduces incentives for incumbent companies to innovate.
- Increase vendor lock-in, driving up costs. Vendor lock-in can force customers to continue to use these closed systems lest they pay high switching costs to replace their entire network.
- Jeopardize reliability. Should a 5G network rely heavily on closed technology from only one provider, the reliability and trustworthiness of the network is put in jeopardy if the provider becomes unable to maintain these technologies.

In effect, the use of closed systems in telecommunications poses a significant threat to the speed with which the United States can grow a robust domestic 5G commercial ecosystem that is innovative, competitive, cost-effective, and reliable.

In contrast, the use of 5G technologies built around open standards ensures that any company can create 5G offerings that can easily interoperate with any other company's offerings. This means that small startups and incumbent firms alike are on an even playing field and can compete to develop innovative and cost-effective "plug and play" solutions.

The benefits of open standards are particularly evident at radio access network (RAN) layer at the edge of 5G networks. The radio access network relies on several pieces of hardware and software working together to foster connectivity between devices like smart phones, connected vehicles, and sensors and the network core. The use of closed, black-box architectures by some companies prevents their technology from easily, seamlessly, and securely working with technology from any other provider, limiting innovation and competition in the RAN layer.

Fortunately, many in industry are coalescing around the idea that open approaches to 5G are vital to their business, just as they are vital to national security and the economy. For example, IBM has pledged to adopt the Open Radio Access Network (O-RAN) standard, along with many other companies, as the foundation for the critically important RAN layer of 5G networks. The O-RAN standard is a multiplier, enabling exponential growth in 5G by fostering healthy competition in software communities, as contributors define open specifications so that components from different companies can work together to form a "best of breed" solution. Open 5G architectures like the O-RAN standard break down "walled gardens" and drive innovation.

While IBM and other companies are leading the development and deployment of open technologies-based 5G, the U.S. government can help accelerate this transformation by ensuring the National Strategy to Secure 5G, and any future 5G strategies, promote the adoption of open standards. For example, the National Telecommunications and Information Administration should use its convening authority to discuss, report on, and promote open 5G technologies to raise awareness and adoption domestically and globally. Additionally, the Department of Defense should use its procurement authorities to fast-track and give preferred consideration for 5G solutions that utilize open standards, in its 5G infrastructure pilots. And the Federal Communications Commission should encourage industry to only fund the purchase of 5G telecommunications equipment that utilizes open standards.

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

There are many opportunities for the U.S. government to accelerate the research and development of open 5G technologies by industry, research agencies, and academia. These include, but are not limited to:

- Direct financial incentives, such as R&D grants funded by money raised from spectrum auctions or other sources, or low- or no-interest loans for investments in open 5G technologies;
- Tax incentives, such as an increase in the R&D tax credit specifically for investments in 5G R&D; and
- Investments in human capital, such as working with the National Science Foundation to promote the development of skills necessary to develop and work with 5G technologies;

Fortunately, legislative solutions to enact these strategies already exist. Section 501 of the Intelligence Authorization Act for FY2021 and the bipartisan U.S.A. Telecommunications Act (H.R.6624) would make a substantial amount of funding available to accelerate the research and development of open 5G technologies.[1] The administration should work with Congress to pursue a diverse portfolio of strategies to foster and promote the research and development of new and open 5G technologies and architectures.

(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.

[1] https://www.congress.gov/bill/116th-congress/senate-bill/3905/text, https://www.congress.gov/bill/116th-congress/house-bill/6624/

As described above, the best way to encourage the private sector to invest in 5G technologies is to encourage the widespread adoption of open standards. When incumbents with large market share rely on closed systems to prevent interoperability and create high switching costs, small and large companies alike face high barriers to entry. By contrast, a 5G ecosystem built around open architectures would create a robust and competitive marketplace in which firms of any size can carve out market share with innovative new offerings.

The U.S. government should also strive to foster competition and consumer choice throughout the 5G ecosystem. For example, the government should seek to eliminate barriers to telecommunications customers implementing or transitioning to open source-driven cloud technologies, which can provide customers with greater control, stability, and resiliency.[2]

Line of Effort Two: 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?

There are several factors the U.S. government should consider. First, the government should use the widely accepted Prague Proposals as a foundation for its approach to 5G security.[3] Second, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has launched a project to work with industry to develop a NIST Cybersecurity Practice Guide, which will serve as a public resource to provide guidance about 5G cybersecurity. Traditionally, cybersecurity is addressed by assessing risk and using risk management practices and frameworks, and 5G infrastructure is no different. For example, whether it is applying the foundational NIST Framework for Improving Critical Infrastructure Cybersecurity to the 5G environment or promoting Charter of Trust's Responsibility Throughout the Digital Supply Chain to address IoT security concerns with baseline security requirements for suppliers, both are rooted in public private partnerships and risk management that are transferable to the 5G environment.[4] Overall, as various industry groups, government agencies, and other stakeholders continue to develop cybersecurity resources for 5G, the government should be careful to avoid additional burdensome, prescriptive rules while developing guidance built around international standards and best practices for cybersecurity.

(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?

[2] https://www.ibm.com/blogs/policy/open-5g-pov/
[3] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/
[4] https://www.charteroftrust.com/topics/

A key factor that the U.S. Government, along with other stakeholders, will have to consider is what is actually meant by the term "5G infrastructure." While 5G entails similar kinds of telecommunications infrastructure as prior generations of wireless technology, it also includes an unprecedented amount of software and is much more reliant on newer technologies like cloud computing to manage network functions. As such, the line between the infrastructure layer and application layer in 5G is blurred. Industry and government in the United States and abroad should agree on a common model that clearly defines what 5G infrastructure entails and use existing global standards to evaluate and develop secure 5G infrastructure. That being said, the government should leverage the work being conducted by the Department of Homeland Security's (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force and its Tiger Team's inventory of supply chain government programs, legislation, and industry efforts to illustrate the ecosystem of efforts addressing supply chain issues.

(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?

As mentioned previously, the government should leverage the work group products from the DHS ICT SCRM Task Force, as much of it focuses on risk-based decisions for procurement and is intended to feed into the new Federal Acquisition Security Council's decision-making processes. For example, the government should consider promoting the work of the DHS ICT SCRM Task Force and the qualified bidder/manufacturing lists (QBL/QML) to inform the policy and procurement community on qualification criteria and expectations for 5G infrastructure.

(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?

The government should incentivize industry adherence to existing security standards, such as ISO 27000 series, ISO/IEC 27036, and ISO/IEC 20243, by granting safe harbor for parties that demonstrate good faith in adhering to these standards.

Line of Effort Four: 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?

As described above, the widespread adoption of open standards in the United States and by trusted international partners is the key enabling factor in fostering the development of a robust international marketplace for innovative, secure, and reliable 5G technologies.

(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 should develop a shared funding vehicle cooperatively supported by and administered with trusted international partners to provide financial incentives for the deployment of secure and open 5G technologies. The Intelligence Authorization Act for FY2021 would create such a fund, called the Multilateral Telecommunications Security Fund. This fund would be a common funding mechanism run by the State Department in coordination with foreign partners to support the development and adoption of trusted telecommunications technologies.[5] Ideally, this fund would also be paid into by trusted international partners as a condition for their domestic companies to be eligible to receive grants from this fund, and these funds should only be made available for deployments that utilize open standards wherever appropriate.

Once again, IBM appreciates the opportunity to comment and we look forward to future engagements. For any questions, please contact Mr. Joshua New at Joshua.New@ibm.com

Sincerely,

Roslyn Docktor
Director, Technology Policy
Government and Regulatory Affairs

[5] https://www.congress.gov/bill/116th-congress/senate-bill/3905/text