Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	)	
	)	
National Telecommunications and Information Administration, requests for comments on the National Strategy to Secure 5G Implementation Plan	)	Docket No. 200521-0144

COMMENTS OF
BLACKBERRY CORPORATION

BlackBerry Corporation[1] respectfully submits these comments in response to the National Telecommunications and Information Administration (NTIA), request for comments on the National Strategy to Secure 5G Implementation Plan. Innovation within telecommunications and software is taking place at a rate never seen in history. The promise of 5th Generation Telecommunications will power smart cities, autonomous vehicles, increase the speed of commerce, and enable the access to advanced technologies; therefore, BlackBerry is grateful for the opportunity to provide input into such an important effort.

Public Law 116-129[2] provides the administration – and in-turn NTIA – a unique place in history; to publicly create and structure a foundation for the future. Regardless of the infrastructure constructed, if it is not secure from inception it will not live up to its promise and potential; nor will it meet the challenges of future technologies. BlackBerry encourages the continued engagement of all elements of national power and security; to include the Department

[1] BlackBerry Corporation has provided secure communications to the world governments and largest businesses for over 35 years. From secure devices, we have shifted that technology to build some of the worlds most advanced cybersecurity technologies, utilizing Artificial Intelligence (AI) and Machine Learning (ML) to ensure zero-trust environments for some of the most critical operations. This combined with BlackBerry's work on secure real-time operating systems that power everything from 175 vehicles worldwide, to vital observation equipment on the international space station, places our company in a unique position as a software provider that offers operational effectiveness with security into the very design of our products and services.

[2] https://www.govinfo.gov/content/pkg/PLAW-116publ129/html/PLAW-116publ129.htm

of Defense, The National Security Administration, the Department of State, the Department of Homeland Security, and the Department of Energy; as well as, the knowledge and power of American private industry; allied nations; and their private industries. The use of international standards bodies and increased science and technology investment will aid our nation in these efforts and ensure leadership in telecommunications.

In our below remarks we only answer questions from Docket No. 200521-0144 that meet with BlackBerry's expertise; therefore, the parenthetical numbers referenced under the *Lines of Effort* are not ordered but rather references to docket questions, as referenced in the ***Federal Register.***[3]

I. LINE OF EFFORT ONE: FALCILITATE 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)?

From a software perspective there are three key elements that would aid in the implementation and advancement of 5G. First, the current and continued efforts to keep private industry, including the software industry, as part of the conversation. We applaud the foresight of the administration to ensure private industry has a voice in this effort. Second, ensuring embedded systems are designed with over the air update capabilities and high security standard conformance. This will lay a foundation for continued secure software development. Risk

[3] *'the Docket' and 'Federal Register'* in this document refers to ***Federal Register*** */ Vol. 85, No. 103 / Thursday, May 28, 2020 / Notices;* ***Department of Commerce****, National Telecommunications and Information Administration [Docket No. 200521] RIN 0660-XC047 National Strategy to Secure 5G Implementation Plan.* https://www.ntia.gov/files/ntia/publications/fr-secure-5g-implementation-plan-05282020.pdf

mitigations in software begin with an operating system that is secure, versatile, and continually updated. The operating system must meet the highest international standards for safety, such uniform standards allow software developers to build, grow, and improve solutions in certain devices (e.g., automotive)[4]. Finally, the systems within a 5G network should designed with a zero-trust architecture, which requires continuous authentication and validation from endpoint to endpoint, ensuring the end-to-end security that is imperative to the end users.

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

BlackBerry recommends that the Administration encourages and supports participation in international standards organizations. Such participation provides insight, lessons learned, and enhanced business practices for U.S. companies and Government departments. Although the United States leads in many organizations, we are the smallest participant in the umbrella organization for 5G development. Presently American participation in the 3rd Generation Partnership Project (3GPP) is 8% of total participation.[5] This means, that at present Asia and Europe have a larger voice in setting 5G standards for the world. It also means that the United States is being largely left out of the discussion and the transfer of lessons from the other participants.

[4] *BlackBerry Ultimate Guide to Embedded Systems Security* https://blackberry.qnx.com/en/embedded-system-security/ultimate-guide/

[5] https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_87E_Electronic/Docs/SP-200127.zip)

(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.

Many of the challenges among existing technologies that would utilize 5G are limited by their ability to share spectrum. Applications, such as Vehicle to Everything (V2X), are battling between technologies to retain control of spectrum channels;[6] this creates a failure in the ability for technologies to compete in the market. Instead, they compete in a non-competitive pre-market environment. Because of this, BlackBerry supports government promotion of further research in **spectrum sharing**. The importance of this research is the ability to build on longitudinal studies that provide academics with the ability to conduct deep research; as well as provide private companies an offset of risk for long-term products that do not show an early market value.

II. 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?

The supply chain for 5G will be one of the most diverse in the world. Silicon, devices, applications, and software all create compounding vulnerabilities. Tracking, tracing, and

[6] *FCC Seeks to Promote Innovation in the 5.9 GHz Band*, Federal Communications Commission, Dec 19, 2019 https://www.fcc.gov/document/fcc-seeks-promote-innovation-59-ghz-band-0

verifying these products will differ from hardware to software. However, some basic security levels should be required from manufactures, regardless of type. For example, manufacturers should meet minimum levels of security practices and audits for critical infrastructure. Utilizing the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* provides a baseline for key internal controls. Inherent in this is the ability to maintain a robust insider threat program[7] ensuring that vulnerabilities and *backdoors* are not build into the system. Technologies which require continuous and automated authentication and zero-trust architecture aid in this process. Therefore, BlackBerry suggests encouraging standards development for zero-trust to ensure the application of artificial intelligence technologies and other advanced technologies as part of the security solutions development.

Also inherent within the framework is the need for a robust supply chain risk management system (SCRM).[8] To truly trace and track an entire supply chain for a product a manufacturer must be able to maintain a serialized track and trace (STT) process. A secure and effective way to do this is through unique cryptographic keys injected into each device, providing a secure means by which each unique manufactured element can be individually tracked, and verified. For software developers, full vulnerability scans must be completed. This is especially important when source code is not fully availed; a focus on **binary static analysis tools** can aid, along with sound cyber business practices, to ensure the security of the software supply chain.

---

[7] *Framework for Improving Critical Infrastructure Cybersecurity*, Page 27, NIST April *16*,2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[8] *Framework for Improving Critical Infrastructure Cybersecurity*, Page 15-21, NIST April *16*,2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

(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?

As mentioned previously, BlackBerry applauds the work done by NIST and its contributors; therefore, we recommend the development of a NIST Framework for 5G security. Such framework would outline 3rd party audit requirements. BlackBerry supports the Cyberspace Solarium Commission's (CSC) recommendations on increased reporting requirements, public-private coordination, and *Whole-of-Country* approach to critical infrastructure security [along with many other recommendations presented by the group].[9] In March of 2020 the CSC released a report citing 5G as one of the *trends* that are reshaping the cyberspace, and driving the need for more advanced security measures. The administration should consider utilizing the full power of government regulation to ensure high standards of security and reporting, as discussed in the document. The administration should also consider increased stakeholder contributions and public-private partnerships to ensure a full understanding and shared responsibility for network security. Also, prominent in the CSC report is the need for strong allies in developing a security system. As such, co-developing reporting and security standards with allied governments would ensure businesses a streamlined approach to security; and provide government assurance that products and services across borders meet the same standards for security and privacy protection.

[9] *Cyberspace Solarium Commission Final Report*, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

III. LINE OF EFFORT THREE: 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 increase in data rates and decrease in data costs of 5G networks encourage new use cases and subsequently increase the rate of innovation. As pointed out in a paper presented by the Information Technology and Innovation Foundation (ITIF) 5G is the next step in a cycle of *dizzying innovation* that began with 4G and LTE.[10] Future updates to 5G will enable digitization in new verticals including enhancements to automotive safety and efficiency. The initial advancements in V2X technologies can move beyond basic safety messaging to providing full advantages to automated vehicles aiding in the reduction of traffic issues, improved energy savings, safety, and – as a value to all industries – increased reliability of logistics systems. Widely deployed sensors will make agriculture more efficient through shared sensor data and on the edge AI, which will deliver needed nutrients to crops under optimal conditions; and therefor increase yield. Medical information will be less costly to collect, and analyze, and share in a secure manner improving patient outcomes. The values to public good, national defense, and economic growth are innumerable with more versatile networks. However, this is only possible if data and privacy are secure and if its effects extend beyond one country. A lack of universal standards or a system built on vulnerability will stunt 5G potential.

[10] *A U.S. National Strategy for 5G and Future Wireless Innovation*, Information Technology and innovation foundation. https://itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation

IV. LINE OF EFFORT FOUR: PROMOTE RESPONSIBLE GLOBAL DEVELOPMENT AND DEPLOYMENT OF 5G.

(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?

To optimize risk mitigation BlackBerry recommends a multi-tier approach. This begins with secure supply chain management, through a thorough STT system and software lifecycle management through binary static analysis tools. It continues with network security. This includes secure 5G network management, operation, and monitoring. [For example, session control and traffic flow management signaling at the interworking gateways.] Finally, it requires security at the software level beginning with secure embedded operating systems and protected external endpoints, and then ensuring security within the system utilizing a zero-trust architecture that is enabled by behaviorally based machine learning that can rapidly adapt rules based on threat.

We recommend a series of traditional as well as peer-based models to measure success. For example, number of breaches per intrusion attempts, mean-time-to-contain, mean-time-to-detect, and comparing these metrics state-to-state, as well as country-to-country. It is important that the comparison is not seen as a competition between allies, but as a level of information sharing that is designed to build better practices and lessons learned daily.

V. CONCLUSION

BlackBerry appreciates the opportunity to offer our recommendations to NTIA and we applaud the foresight of the administration in their early collaboration with industry on the matter of 5G security. As we conclude we would like to reiterate that we believe 5G is one of the base

technologies that will change the way people function in the world, and that it is only through cooperation, standards, and security that we will meet our full potential.

Respectfully submitted,

BLACKBERRY CORPORATION

By:_____

Jeffrey W. Davis Jr.
Sr. Director Government Affairs &
Public Policy

BlackBerry Corporation
3001 Bishop Drive
San Ramon, CA
(877) 255-2377

June 25, 2020