TOSHIBA

QUANTUM XCHANGE

June 19, 2020

Mr. Douglas Kinkoph
Associate Administrator
Office of Telecommunications and Information Applications,
Performing the Delegated Duties of the
Assistant Secretary of Commerce for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Re: Comments of Toshiba Corporation and Quantum Xchange, Inc. in response to NTIA's Request for Comments to inform the development of an Implementation Plan for the National Strategy to Secure 5G, Docket No. 200521-0144

Dear Associate Administrator Kinkoph,

Please accept these Joint Comments filed on behalf of Toshiba Corporation[1] (Toshiba) and Quantum Xchange[2] (QXC) (collectively, Joint Commenters) in response to the National Telecommunications and Information Administration's (NTIA) Request for Comments (Request) regarding The National Security to Secure 5G Implementation Plan. As industry-leading companies in the field of quantum-safe security, the Joint Commenters welcome the opportunity to provide comments on the importance of understanding and caring for the threat to 5G networks posed by quantum computers.

5G will materially change telecommunications and with it our way of life by affecting the way people interact with and rely on technology. This is because 5G represents more than a network technology. Rather, it will "become the underlying fabric of an entire ecosystem of fully connected intelligent sensors and devices." [3] Examples of such intelligent sensors and devices

[1] Toshiba Corporation is headquartered in Tokyo, Japan. Toshiba and its predecessor companies have been in business since 1873 and have developed numerous pioneering electric and electronic products that represented the first of their kind in Japan or anywhere in the world.
[2] Established in 2018, Quantum Xchange, Inc. is headquartered in Bethesda, Maryland. Quantum Xchange is an industry leader in the nascent field of quantum encryption technologies and is the first company in the world to offer quantum key distribution on a commercial basis.
[3] TR Staff, *The 5G Economy: How 5G Will Impact Global Industries, the Economy, and You*, MIT Tech. Rev. (March 2017)

range from industrial sensors to medical devices to autonomous vehicles. As one expert explains, "5G shifts communications to a computing platform." [4]

As this paradigmatic shift occurs, our reliance on 5G technology grows and with it our vulnerability to cybercriminals and other nefarious actors. The promise of the benefits associated with autonomous cars, robotic surgery, and enhanced smart grids for utilities is revolutionary but will only be viable if those platforms can be kept safe. In the hands of individuals and/or nation states with malicious intent, the results could be devastating.

At the same time that 5G networks are being developed, another technological advance promising equally dramatic change is also emerging – quantum computing. Quantum technology will introduce a level of computer power and sophistication greatly surpassing the capabilities of existing computing. This includes, notably, the ability to render useless the traditional public-key infrastructure (PKI) ciphers currently used to protect virtually all forms of networking, including 5G.

While there are those who question the urgency of the quantum threat, the reality that quantum computing is developing at a rapid pace is beyond dispute. In October, 2019 Google announced that it had achieved "quantum supremacy" i.e., when a quantum computer performs a task a classical computer cannot perform.[5] Moreover, at least one major computing manufacturer expects that quantum computing will become mainstream in the next five years[6] while other industry participants have suggested that classical-quantum computing hybrids will be viable in two years.[7]

But even putting those predictions aside, the fact is that in anticipation of the arrival of quantum computing, attacks have already begun threatening computer network security. These attacks are commonly referred to as "harvesting" attacks. Harvesting attacks involve a relatively unsophisticated level of eavesdropping on communications links and the recording and storing of the data in transit (including the security keys). Once the requisite level of computing power exists to break the keys, the data will be "harvested" to reveal the secrets contained in the transmission.

[4] Darrell M. West, *How 5G Technology Enables the Health Internet of Things*, Ctr. for Tech. Innovation Brookings (July 2016)

[5] Arute, F., Arya, K., Babbush, R., *et al.*, *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 Nature 505 (2019) available at: https://doi.org/10.1038/s41586-019-1666-5

[6] *5-In-5 Five Innovations That Will Help Change Our Lives Within 5 Years*, available at: https://www.research.ibm.com/5-in-5/quantum-computing/

[7] Kristen LeBlanc, *Quantum Computing: How Soon Will It Become a Mainstream Reality?* available at: https://atos.net/en-na/north-america/quantum-computing-how-soon-will-it-become-a-mainstream-reality-t

It is for all of these reasons that NTIA's line of inquiry regarding assessing risk and identifying core security principles of 5G is so important. Recognizing the emerging threat to PKI, the National Institute of Standards and Technology (NIST) announced an initiative in 2016 which is still ongoing to develop post-quantum cryptographic (PQC) algorithms as alternatives to current PKI ciphers.[8]

There exists a critical need to ensure that 5G standards address the quantum threat and support the development of alternatives to PKI ciphers.[9] Moreover, it is important that NTIA recognize that all forms of quantum-safe security have unique merits and limitations and as a consequence, cybersecurity best practices dictate the use of multiple forms and layers of protection.

As a result, the Joint Commenters believe that 5G ecosystem participants must adopt a posture of quantum readiness and defense-in-depth countermeasures to address the challenges quantum computers will pose. We urge NTIA to refrain from mandating the specific type(s) of post-quantum protection for 5G networks. Instead, the Joint Commenters support steps by NTIA to encourage a focus on crypto-agility that will enable 5G network providers to deploy quantum-safe alternatives in advance of the emergence of quantum computing and to adjust to threats as they develop.

NIST, as part of its work on quantum security, has acknowledged that maintaining a focus on crypto agility is imperative.[10] The Joint Commenters applaud NIST's crypto-agility efforts as they pertain to PQC standardization, but we also believe that effective crypto agility must be comprehensive and promote important cybersecurity principles such as defense-in-depth.[11]

Defense-in-depth is a well-established means of protecting against hacking threats that incorporates multilayered security with redundancy and diversity. In the case of 5G networks, a defense-in-depth approach translates to the use of various types of post-quantum protections across the entire 5G ecosystem. These may include quantum security schemes that are physics-based like Quantum Key Distribution (QKD) or quantum random number generators (QRNG) as

[8] Lily Chen et al., *Report on Post-Quantum Cryptography*, NISTIR 8105 (2016) (*NIST Report*) available at: http://dx.doi.org/10.6028/NIST.IR.8105

[9] T. Charles Clancy, Robert W. McGwier & Lidong Chen, *TUTORIAL: Post-Quantum Cryptography and 5G Security*, In WiSec '19: ACM Conference on Security and Privacy in Wireless and Mobile Networks (2019) available at: https://doi.org/10.1145/ 3317549.3324882

[10] *NIST Report* at 7

[11] To date, the majority of NIST's focus has been on the development of post-quantum cryptographic algorithms. The Joint Commenters acknowledge that this is a logical first step recognizing that currently the predominant form of public encryption, PKI, is mathematically based. Nevertheless, there are other potential solutions to this problem and more under development. These include the application of physics-based solutions such as the use of QKD systems and the use of QRNG to provide quantum security.

well as mathematical ones. Indeed, it is this type of broad-based approach that is currently the subject of trials by U.S. allies[12] as well as its rivals.[13]

Accordingly, the Joint Commenters recommend that NTIA avoid mandating a particular form of post-quantum security based on the current state of research by NIST which has focused almost exclusively on PQC algorithms. Rather, NTIA is encouraged to permit participants in the 5G ecosystem to select the quantum-safe technology that they believe most appropriately addresses the threat – whether that be a more traditionally oriented solution or one from the panoply of emerging technologies.

An added benefit of NTIA adopting a fit-for-purpose approach to 5G security is that such an approach maintains the incentives for the development of new, perhaps even currently unimagined, solutions to be developed in the future. Experience in cybersecurity demonstrates that as new threats to a technology evolve, in this case 5G, myriad new defenses will follow.

Indeed, in the last month a major device manufacturer has taken an unprecedented step by incorporating a physics-based solution to protect 5G handsets.[14] This development is clearly a move to create a competitively differentiated product by touting quantum security and reasonably can be expected to be only the first of many such moves across the 5G ecosystem. By embracing the level of post-quantum security flexibility the Joint Commenters suggest, NTIA will leverage market forces to their fullest extent to promote the development of safe, efficient security solutions.

The Joint Commenters appreciate the opportunity to participate in this important initiative. The implementation of 5G networks stand to usher in a wealth of new applications, ingenuity and economic growth. For that potential to be fully realized, however; the 5G ecosystem must be

[12] *Implementation Security of Quantum Cryptography Introduction, Challenges, Solutions*, First Edition ETSI White Paper No. 27 at 11-12 (2018) available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf "It is very likely therefore that QKD, quantum random number generation and other quantum-based primitives, will be used in conjunction with quantum resistant algorithms in future quantum-safe infrastructures." *See also*, https://openqkd.eu/openqkd-in-action/ Interoperability of QKD and PQC using 5G and fiber link (Use-Case 27) which "proposes an integration of core fiber and 5G access networks, where the fiber sections are secured by QKD and the 5G services are secured by post-quantum cryptography (PQC). "

[13] Feihu Xu et al., *Secure Quantum Key Distribution with Realistic Devices*, 92.2 Rev.s Mod. Physics 3 at 3 (2020), available at: https://arxiv.org/abs/1903.09051 "we believe that the two approaches - post-quantum cryptography and quantum cryptography - are *complementary* to each other (rather than mutually exclusive)."(emphasis in original)

[14] Davey Winder, *Samsung Surprise as World's First Smartphone with Quantum Technology Launches May 22*, Forbes, available at: https://www.forbes.com/sites/daveywinder/2020/05/15/samsungs-surprising-new-5g-smartphone-is-worlds-first-with-quantum-technology/#71b2812030e0

TOSHIBA

QUANTUMXCHANGE

secure from both existing and emerging threats – particularly quantum computing. The Joint Commenters encourage NTIA to adopt policies that encourage 5G ecosystem participants to adopt a cyber-agile posture and which enable those participants to craft the best cybersecurity solution for their unique needs from the widest range and combinations of quantum-safe solutions.

Respectfully submitted,

Taro Shimada
Corporate Senior Vice President
Toshiba Corporation

John Prisco
President and CEO
Quantum Xchange, Inc.
7700 Old Georgetown Rd.
Suite 850
Bethesda, MD 20814