June 18, 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 NW
Washington DC 20230

Re: Comments of the Quantum Industry Coalition 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,

I am the Executive Director of the Quantum Industry Coalition (QIC), a group of companies dedicated to U.S. leadership in the quantum fields. Its members include Accenture, AgilePQ, Bra-Ket Science, ColdQuanta, D-Wave Government, EeroQ, Entanglement Institute, Founders Fund, IBM, Intel, MagiQ Technologies, Nanotronics, Quantum Xchange, QxBranch, Rigetti Computing, StrangeWorks, Turing Inc., Xofia, and Zapata Computing. I am writing on behalf of QIC in response to the National Telecommunications and Information Administration's (NTIA) Request for Comments (Request) regarding the National Strategy to Secure 5G Implementation Plan (Plan).

QIC believes that any strategy to secure 5G must take into account the threats and opportunities posed by quantum technologies. We must act now to "future-proof" 5G networks against capabilities that are still on the horizon. The comments below are directed primarily in response to the questions posed by the Request within line of effort #2, "assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure."

Quantum computing has the potential to defeat the public-key infrastructure (PKI) ciphers on which nearly every network currently relies for security. Because 5G also relies on PKI ciphers, it is vulnerable to a future quantum attack. A quantum attack could include exploits at the hardware, infrastructure, encryption, and software levels, and so each must be protected.

QIC strongly recommends that the Plan take into account post-quantum security from the start. In other words, the Plan should promote an architecture that allows for security protocols that are no more vulnerable to quantum computers than they are to classical computers. Lattice-based and multivariate public-key cryptography are examples of potentially viable solutions, as could be Quantum Key Distribution (QKD).

Post-quantum security standards are under discussion under the purview of NIST, and QIC recommends that the Plan prioritize enabling 5G networks to switch to post-quantum security after installation.

It is vital to protect 5G network backhauls from cable-sniffing and other attacks. It is important to do this immediately, even though quantum computers cannot yet defeat PKI, because attackers are already accessing encrypted data for storage and later quantum decryption.

The early stage of quantum development also underscores the importance of avoiding technology mandates in the Plan, and of refraining from picking winners and losers in the marketplace. Post-quantum security must be allowed to develop organically, and the owners and users of 5G networks should have access to the latest and best security options rather than being tied to an outdated government-required standard.

Although inter-hub backbone cabling is amenable to QKD, commercial QKD systems are currently under development for full deployment across communication networks. We suggest a strategic research and development focus on creating QKD technologies for networks like the fiber backbone for 5G to be addressed with future government funding. Proof of concept deployments of probable QKD network requirements should be conducted to see if there are recommendations that can be made to assure any hardware upgrades have a greater probability of meeting future QKD technology needs. Defense-in-depth approaches that combine Post Quantum Cryptographic algorithms with QKD should be explored in the US as they are currently in Europe and China.

Among the stakeholder-driven approaches that the U.S. Government should consider with respect to the post-quantum security aspects of 5G infrastructure are efforts currently underway through the National Institute of Standards and Technology (NIST) on post-quantum cryptography. Additionally, quantum communication technologies to be developed within National Quantum Initiative (NQI) research programs through the Department of Energy and National Science Foundation, as well as ancillary technologies to be developed through the Quantum Economic Development Consortium under the auspices of NIST, should be coordinated to address this national challenge. These NQI initiatives involve a whole-of-nation approach, involving all stakeholders, including government, industry, academia, and thought leaders like the Quantum Alliance Initiative at the Hudson Institute, as well as collaborations with friendly foreign institutions and initiatives. Key to any stakeholder process is substantial input from the private sector, where quantum technologies and post-quantum security capabilities are being developed and deployed.

Within the Government, NTIA should engage with the National Quantum Coordination Office in the Executive Office of the President, and with the Assistant Director for Quantum Science in the office of the Under Secretary of Defense for Research and Engineering.

One of the best ways that the U.S. Government can promote the adoption of policies, requirements, guidelines, and procurement strategies necessary to establish secure, effective, and reliable 5G infrastructure is by consistently being a first customer. In doing so, the Government should:

- operate on a tempo approximating that of business;
- avoid needlessly complicated purchasing processes and contracts;
- minimize compliance costs; and
- handle intellectual property issues fairly, smoothly, and consistently.

In addition, the Government should consider refusing to participate in communications regimes that do not meet post-quantum security standards.

Thank you for your attention to these important matters.

Sincerely,

Paul Stimers
Executive Director
Quantum Industry Coalition
www.quantumindustrycoalition.com