Q Networks, LLC

3617 Oak Dr.
Menlo Park, CA 94025-1950
650-704-2326

Travis Hall **Date: June 18, 2020**
Telecommunications Policy Specialist
Office of Policy Analysis and Development
National Telecommunications Industry Association (NTIA)

United States Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

Re: *Docket No. 200521-0144, Request for Comments on National Strategy to Secure 5G Implementation Plan*

5G technology will redefine the future of computing and catalyze unprecedented economic growth and innovation for the world. The low-latency, high-bandwidth capabilities and service-oriented architecture of 5G networks will become the foundation for emerging technologies, especially applications that will enable massive machine-to-machine communications such as industrial IoT, artificial intelligence, and driverless vehicles.

To enable these transformative technologies, the mobile network market is evolving rapidly. The U.S. Government's allocation of unlicensed mobile spectrum has enabled large organizations to shift away from traditional telecommunications operator-controlled public networks that were built for consumers to private networks that they can control and maintain. The future of mobile networking will be hybrid mobile networks that consist of private 5G wireless infrastructure in government/enterprise-controlled areas and public LTE/ 5G networks that provide roaming coverage wherever private networks are not available.

The U.S. Government should encourage the deployment of a network architecture that is both flexible and conducive for rapid innovation while being highly secure. Telecom standards group, 3GPP, and their 5G architecture has not kept pace with current innovations in cloud architecture over the past decade. Cloud architecture concepts such as Virtual Private Clouds (VPC) that allow applications to create their own highly customizable, private virtual infrastructure that can be controlled and secured according to the needs of the application have not been adopted given 3GPP's focus on legacy telecom carrier infrastructure. 3GPP's standards still offers a common mobile network that all enterprise applications and devices are connected to, rather than application-specific customizable networks that are self-provisioned, controlled, and secured by enterprise applications.

The evolution of 3GPP standards from LTE to 5G was driven primarily by a motivation to preserve substantial capital investments in legacy networks and to use the cloud integration merely for cost optimization. Today, the fundamental architecture of 5G networks is no longer suited to provide government-grade or enterprise-grade security for data and communications.

The following are examples of critical architectural and security issues that need to be addressed in any 5G network architecture designed to support critical data or communications:

- Network slicing has enhanced the "one-size-fits-all" approach to network design of LTE to a "few-sizes-fit-all" approach, but this falls well short of the standard for application infrastructures today – the Virtual Private Cloud (VPC) paradigm of clouds.
- Inability to deal with scalability, reliability, and redundancy, and assuredly leverage legacy architecture.

- Expanding attack surfaces due to unsecure microservices based architecture.
- Limited or weak standards to secure interfaces between network functions, components, and subsystems in addition to lax and unenforceable processes and standards for trust between operators.
- Network slicing issues:
  - Lack of standards for isolation between network slices.
  - Slices are likely shared between customers, depending on operator defined service architecture.
  - Common control plane across all network slices.
- Lack of data sovereignty for customer subscription data without risk of exposure in carrier networks.

There is an urgent need for the United States to establish leadership in 5G by creating a secure standalone state-of-the-art 5G network for the military, intelligence, and commercial entities. The United States cannot rely on the current market players to drive this critical initiative.

The U.S. Government can address the global economic and security risks presented with 5G use by ensuring that an end-to-end American solution exists and should incentivize and foster competition in the telecommunications marketplace. The U.S. Government is uniquely positioned to utilize government contracts to stimulate the market, drive demand, and bring the per unit cost down to a competitive price of network solutions, while ensuring security principals in the best interest of its citizens are prioritized and maintained.

The U.S. Government would be prudent to only do business and operate with vendors that support counterintelligence programs, principles of nuclear surety, and zero trust security best practices and it must ensure that all existing and pending technology contracts are aligned with a secure, American-sourced 5G network enablement strategy. These initiatives, specifically, are critical when evaluating security gaps in 5G infrastructure. Furthermore, stakeholder-driven approaches that the U.S. Government should mandate in all government technology contracts include zero trust security and American-sourced end-to-end solutions.

With a homegrown, end-to-end secure 5G solution, the innovative solutions that emerge because of 5G enablement will demonstrate the value of a secure network to the global marketplace, and continue to showcase the United States as a global leader for years to come.

Appendix A: Responses to Questions for Comment

Line of Effort One: Facilitate Domestic 5G Rollout

7. 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)?
    - A paradigm shift in end-to-end network security architecture is needed because the existing model for a non-standalone architecture is inherently unsecure. There is an urgent need for the United States to establish leadership in 5G by creating a secure, standalone, state-of-the-art 5G network for the military, intelligence, and commercial entities. The United States cannot rely on the current market players to drive this critical initiative.
8. 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 is uniquely positioned to utilize government contracts to stimulate the market, drive demand, and bring the per unit cost down of network solutions to a competitive price, while ensuring security principals in the best interest of its citizens are prioritized and maintained. Additionally, the U.S. Government should use the development of finance for U.S. solutions to promote a secure end-to-end 5G network solution and allocate a portion of the federal budget to basic science research to explore additional use cases of 5G technology. The government needs to encourage investments in foundational and basic 5G research. The public-private-academic partnership model that the U.S. pioneered must be reinstated. Specifically, the government needs to do the following to establish U.S. leadership in 5G:
        - Set-up dedicated funds to drive basic research and innovation in 5G
        - Free up sub-6 spectrum to help drive 5G deployment in rural areas
        - Create dynamic sharing of spectrum or a utilization system that promotes new capital and entrepreneurs
        - Implement a strategy to promote 5G infrastructure development in rural America
        - Reinvigorate indigenous manufacturing of 5G and next-generation telecom equipment
        - Promote a new system of data governance that protects users personal and sensitive data
        - Set up a 5G Implementation Council to coordinate 5G adoption across industry verticals
        - Introduce legislation that makes it easier to deploy 5G infrastructure
        - Pursue a comprehensive program of patent and intellectual property protection.
9. 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 needs to step in and support small businesses in the telecom sector with tax incentives and preferential contracts for small businesses. Benefits beyond awarding Department of Defense SBIR contracts must exist. In order to effectively audit the current support for small businesses in telecommunications and gain clarity on how to best implement programs that support these businesses effectively in the future, an evaluation indicating the percentage of annual telecom spend being awarded to small innovative businesses.
10. 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.

- Radio - Currently, there are very few suppliers. The ecosystem is constrained by the current business environment where the few suppliers that are there are only designing and manufacturing what legacy carriers deem necessary. We need to see R&D investment in the field of ORAN and other software defined radios.
- Antenna – Similar to radio, antenna suppliers are inherently focused on supplying legacy carrier requirements. R&D investment is necessary.
- Computing - Chipset design and manufacturing, as well as general software development, should be bought back to the United States with incentives to invigorate the reindustrialization of these two tech sectors.
- Networking - Basic R&D should be invested in the field of next-generation "open" software designed networks.
- Virtualization - The enterprise software ecosystem has dramatically benefited from virtualization, as has the enabling of application developers. Further advancement in this field, applied to telecom, is necessary.
- Spectrum – It is necessary that additional spectrum is opened and made available for public use, especially compared to the current acquisition model.
- Security – U.S. citizens' data is the oil of the next generation. For the U.S. to remain sovereign and ensure that democracy thrives into the future, there must be protections of digital environments, experiences, and identities. Government-level investments must be made in R&D of this digital space and more sophisticated legislation must be advocated and explored to provide guidance on how U.S. citizens data is used and what requires development.

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

11. What factors should the U.S. Government consider in the development of core security principles for 5G infrastructure?
    - 5G technology will redefine the future of computing and catalyze unprecedented economic growth and innovation for the world. The low-latency, high-bandwidth capabilities and service-oriented architecture of 5G networks will become the foundation for emerging technologies, especially applications that will enable massive machine-to-machine communications such as industrial IoT, artificial intelligence, and driverless vehicles.
    - 5G is not an incremental change over its predecessor, 4G. 5G architecture is a redesign including many important technology innovations that move intelligence into the network, transforming the network from a transport pipeline to an entirely new computing platform.
12. 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 internet's original protocols were designed to facilitate communication between a few hundred academic and government users. The internet's design was optimized to move data from one computer to the other and was indifferent to whether the information packets added up to a malicious virus or a video. Nor did it accommodate nodes that moved and could connect from remote locations.[1]

[1] *"The Internet is Broken," MIT Technology Review*

- The U.S. Government must consider all of the potential economic and political priorities of existing vendors in the telecommunications industry. Legacy telecommunications providers have no incentive and do not want to build an entire network architecture as it would discontinue demand for existing product lines and services. Existing vendors are motivated to leverage legacy systems and architecture in new 5G network deployments as much as possible. However, if 5G networks are deployed that leverage any legacy components, legacy security issues will also remain.
- Today, the United States does not have a single 5G equipment manufacturer. Moreover, existing telecommunications operators are building networks with open security philosophies that would personalize the Internet at the expense of citizen privacy and autonomy and result in compromised national security.
- Mobile operators such as AT&T, Verizon, T-Mobile, and Sprint are significant stakeholders in the next generation of network deployments. However, these operators continue to struggle to define and justify the return on investment (ROI) for 5G. Cautiously, these operators are leveraging the market buzz of 5G and are incrementally rebranding their 4G networks as 5G capable or 5G ready.
- Between 2010 and 2017, the U.S. operators invested over $250B in mobile networks. However, these massive investments have not panned out for U.S. operators. Over the last decade, the U.S. operators have suffered declining revenues, cash flow, and return on investment.[2] At the same time, technology/internet companies have thrived by building their businesses on the backs of the operators' infrastructure. Considering most critical financial performance indicators, mobile operators have underperformed, and their stocks are under pressure.
- Operators are making strategic moves to diversify core telecommunications services and compete more effectively with technology/internet companies. AT&T's acquisition of DirecTV and Time Warner Cable is an example of this shift in strategy. These massive acquisitions have led to a situation where operators need to service an enormous amount of debt. Hence, the U.S. operators are moving incrementally on 5G deployment and adopting a phased approach. The operators are beginning with a non-standalone architecture (NSA) where 4G and 5G radio access technologies are used in tandem. 4G technology is over a decade old and has well-documented security flaws. This hybrid approach to 5G implementation will expose the U.S. critical infrastructure and data to security risks.
- The internet's shortcomings have given rise to the thriving cybersecurity industry. Today, over 2,000 security vendors are operating in the U.S. alone. The larger the attack surface and the more significant the impact of cyberattacks, the higher the value of the security software. And the 5G architecture will overwhelmingly increase the attack surface, present voluminous vulnerabilities, and increase the threat sophistication. All factors that will further benefit the current cybersecurity players and hence, it is not in their interest to make the 5G network inherently secure.
- Companies such as Google and Facebook have no incentive to develop a secure 5G network with data protection, security, and privacy. Much of the historical success of the internet industry can be attributed to the monetization of user data while riding on top of the massive communications infrastructure investments made by U.S. operators. The more the users and the greater their usage of apps and services, the higher the revenue for these companies. Google and Facebook have mastered this strategy and use the following playbook to increase utilization of their apps and services:

[2] *Activating AT&T Letter*

    - o Give away services for free to attract users (e.g., search, social media, and email)
    - o Gather user data, mine it, and monetize through targeted advertisements
    - o Grow access to user data by expanding into new services (e.g., Google Home, and Nest)
    - o Galvanize competition to invest in upgrading the internet infrastructure (e.g., Google Fiber)
    - o Germinate new services that create more time to use on the internet (e.g., autonomous driving)
  - 98% of Facebook's and 85% of Google's revenue is from advertising, which is driven by extensive mining of user data to understand personas, preferences, and behaviors. It is not in their economic interest to build secure and private communication infrastructure or to change the existing data model.

13. 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?
14. 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?
    - Stakeholder-driven approaches that the U.S. Government should mandate in all government technology contracts include zero trust security and American-sourced end-to-end solutions.
15. 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 U.S. Government would be prudent to only do business and operate with vendors that support counterintelligence programs, principles of nuclear surety, and zero trust security best practices and it must ensure that all existing and pending technology contracts are aligned with a secure, American-sourced 5G network enablement strategy. These initiatives, specifically, are critical when evaluating security gaps in 5G infrastructure.

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

16. What opportunities does the deployment of 5G networks worldwide create for U.S. companies?
    - Humanity is at the cusp of the next technology revolution that will define the geopolitical landscape for decades to come. Failure to establish a leadership position in 5G will put the United States on the backfoot both economically and militarily. With a homegrown, end-to-end secure 5G solution, the innovative solutions that emerge because of 5G enablement will demonstrate the value of a secure network to the global marketplace, and continue to showcase the United States as a global leader for years to come.
17. How can the U.S. Government best address the economic and security risks presented by the use of 5G worldwide?
    - The countries that lead in 5G will lead the world and they will sustain economic and military superiority for decades to come. Unfortunately, the United States has fallen behind China and other countries when it comes to 5G technology. The current ecosystem of telecom operators, internet oligopolies, and cybersecurity companies cannot be trusted to step up and help the United States become the leader in 5G. The incumbents have built their empires on how the system works today and have no incentive or motivation to change the status quo. They continue to pursue their interests rather than solving the exploding security challenges.
    - 5G technology is based on open software standards and has inherent vulnerabilities across the technology stack. These vulnerabilities can be exploited by adversarial nation-states to

cripple the United States' critical infrastructure, steal important information, and compromise the privacy of United States businesses and citizens. Cyberattacks on the United States' critical infrastructure and citizens have escalated in recent years and will increase exponentially as 5G technology continues to advance.

- The security of 5G has become of paramount importance. Although 5G provides security improvements compared to 4G and previous technologies, 5G increases the number of possible vulnerabilities with an exponential increase in the volume of communications as well as the number of devices and the way in which applications utilize the network.
- China is the clear leader in 5G technology in the world. The Chinese company, Huawei, has the largest global market share, and has the largest share of 5G patents, leads important standards-setting bodies, and has signed over 45 agreements globally to trial 5G networks. Chinese leadership in 5G has serious implications for the security and sovereignty of the United States and its allied nations.

18. How should the U.S. Government best promote 5G vendor diversity and foster market competition?
19. 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?

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G

20. 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 address the global economic and security risks presented with 5G use by ensuring that an end-to-end American solution exists and should incentivize and foster competition in the telecommunications marketplace.
    - The U.S. Government must commit to having representatives that actively participate in global standards organizations to help develop, refine, and deploy the use of those standards and then require all government contracts to use those standards.
21. How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies?
22. 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?
23. 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?
24. 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?
25. What other actions should the U.S. Government take to fulfill the policy goals outlined in the Act and the Strategy?