Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

In the Matter of	)	
	)	
The National Strategy to Secure 5G Implementation Plan	))	Docket No. 200521-0144

COMMENTS OF RAYTHEON TECHNOLOGIES CORPORATION

Raytheon Technologies Corporation ("Raytheon") respectfully submits the following comments in response to the NTIA's request for public comments to inform the development of an Implementation Plan for the National Strategy to Secure 5G. As an aerospace and defense company that provides advanced radiofrequency systems for commercial, military, and government customers worldwide, Raytheon has a significant interest in the security of domestic and international 5G networks.

I. 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 U.S. Government can facilitate domestic rollout of 5G for the commercial ecosystem in several ways. These include funding prototype testbeds in markets across the U.S., supporting open architectures, and facilitating standards participation. A key element is the need for a 5G nationwide roadmap or high-level architecture for the commercial ecosystem to follow. This architecture should include elements to make a 5G rollout successful. These include spectrum allocations, identifying key areas where spectrum sharing must occur, coverage in both rural and

urban environments, and international spectrum alignments (operational and regulatory) especially with the 5G Frequency Range 1 ("FR1") bands (sub 6 GHz).

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

Standards support compatibility of multiple vendor systems and are an important part of ensuring the 5G ecosystem evolves to provide the full vision for 5G across the U.S. Even with these standards, a private sector driven approach has the risk of developing incompatible components. Mitigation occurs by supporting open technologies and open architectures across the 5G commercial ecosystem. The ability for the 5G ecosystem to evaluate and test open systems and new technologies and architectures is critical. The U.S. Government can facilitate open system evaluation with the use of prototype testbeds or even prototype cities for these assessments. This open architecture leads to significant commercial investment in many areas such as spectrum sharing techniques. In addition, it sets the framework for advancing spectrum sharing technologies that could be fielded in the future.

(3) What steps can the U.S. Government take to further motivate the domestic-based 5G commercial ecosystem to increase 5G research, development, and testing?

As discussed above in the response to Question 2, having the ability to test components, architectures, systems, and security enhancements provides the 5G commercial ecosystem a way to evaluate their internal R&D efforts against a U.S. Government roadmap. The use of a Government 5G R&D Innovation Fund to help fast track and scale-up promising candidates would encourage both small and large businesses to bring their systems or components for evaluation.

(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.

The alignment of an Innovation Center or Model City with the Innovation Fund discussed in Question 3 above allows the 5G ecosystem to demonstrate 5G commercial innovations, talent, openness, and diversity of ideas. These are the basic components required to attract venture capital investments. An annual list of technologies and areas of interest aligned with the U.S. Government roadmap to support the 5G commercial ecosystem is essential with re-evaluation occurring on an annual basis. Several areas are ripe for evaluation including:

- Open technologies;
- Open architectures;
- Millimeter wave technologies for 5G Frequency Range 2 ("FR2") (6GHz +);
- Early system-level investments;
- Bidirectional spectrum sharing;
- Beyond 5G to next G;
- Network virtualizations to allow software to emulate the performance of specialized hardware;
- End-to-end security;
- Zero Trust Architectures;
- 5G resiliency; and
- Rural versus urban deployments.

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?

5G will be the most significant physical overhaul of our essential telecommunication networks in decades. It will have a lasting impact on our lives, cultures, and the way we do business followed by future versions, 6G to xG. While still important, this upgrade is less about the hardware and is literally a change from a hardware-focused network to a software network. In 2017, the National Security Agency published a review of 5G Security & Privacy[1] as part of their dissemination of technical advancements and research activities in telecommunications and information technologies. As noted in this review, with each new generation of mobile telephony standards, security has become an increasing concern. For 5G, this will be significant as software vulnerabilities are exploited and rapid software upgrades required. A clear direction from the U.S. Government regarding the national security needs for all telecommunication networks is required. The U.S. Government focus should include but not be limited to policy in:

- Securing a cyber-prone software network;
- Discovering vulnerabilities in the network;
- Managing future upgrades to the software networks;
- Securing the devices and applications enabled by the network;
- Detecting devices/applications that are bad actors and isolating them on the network;
- Providing network resiliency; and
- Authenticating device-to-device communications and securing from impersonation or playback to the network.

[1] *5G Security & Privacy*, The Next Wave Vol.21, No. 4, 2017.

(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?

The Defense Innovation Board published "The 5G Ecosystem: Risks & Opportunities for DoD" in 2019.[2] This paper highlighted many of the supply chain risks for operations. As noted in the paper, there are many risks associated with the use of software intensive networks and the devices or applications running on the network. Even if software is analyzed for vulnerabilities, the upgrades to the software will occur automatically providing a mechanism for backdoors and vulnerabilities to populate throughout the supply chain. Many of the U.S. partners and allies are beginning to use components or networks from countries that have a history of using software to infiltrate the network. The U.S. 5G networks will be required to interoperate with these partner networks. This interoperability exposes the U.S. networks to the same issues as if they directly incorporated the components within the U.S. network. The U.S. Government should consider:

- Providing a clear policy and requirement for the 5G supply chain that requires transparent risk analysis for review;
- Investigating techniques for securing the 5G networks when interfaced to unknown networks, both domestic and international; and
- Developing a common architecture to ensure secure data transfers when interoperating across partner and ally networks similar to a "zero trust" architecture.

(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?

5G has multiple use cases each with specific but different technical requirements. This was not the case with previous network instantiations. With multiple use cases, multiple levels of

[2] *The 5G Ecosystem: Risks & opportunities for DoD*, Defense Innovation Board, April 2019.

security may be required. Previous networks were able to prevent attacks in the network with good awareness in the types of traffic on the network. With the plethora of devices and use cases within 5G, this labor-intensive way of securing the network is not feasible for the entire network. Previous networks typically have a fixed number of well-understood connections allowing the use of a common central authority. As a large number of machine-to-machine connections and device-to-device connections come online within the 5G network, the ability for a central authority becomes limited and the central authority requires modifications to allow arbitrary user and edge equipment in the network.

(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?

The President's National Security Telecommunications Advisory Committee ("NSTAC") provided a report to the President on cybersecurity in 2018.[3] In 2020, these recommendations are still valid. As previously noted, the 5G ecosystem challenges traditional network security assumptions. Current procedural activities for rulemaking and laws, established for networks with centralized control, may not be appropriate for networks with large number of edge devices, multiple use cases, and connected/disconnected device-to-device communications. These should be reconsidered or supplemented with other approaches. Private entities are fully aware of the vulnerabilities within their networks but do not always share these vulnerabilities due to economic exposure. Moving forward, this fear must be alleviated and private enterprise must have a way to share vulnerabilities across a stakeholder group that does not impact economic exposure. Key stakeholder approaches should include:

- Starting with a clearly stated policy and requirements for cybersecurity;

[3] *NSTAC Report to the President on a Cybersecurity Moonshot*, November 14, 2018.

- Developing a structure that enables distributed groups of stakeholders across the Government, private industry, and academia, as a minimum, to participate; and
- Ensuring industry has the ability to discuss vulnerabilities and reach economic agreement on how to meet the cybersecurity requirements.

(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?

Yes. Private entities, or network providers, operate in an environment where investments that do not lead to profit are prioritized last. Further, when one provider does not supply the same controls, it weakens the cybersecurity for all providers on the network, even those that do provide the enhanced cybersecurity controls. This creates disincentives for private entities to invest in cybersecurity.

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?

High investments for FR1 (sub 6 GHz) networks are already underway for U.S. partners and allies. This will limit opportunities in the lower frequencies unless cybersecurity is demonstrated as an inherent part of the network. FR2 (6 GHz +) is a growth area for U.S. companies.

(2) How can the U.S. Government best address the economic and national security risks presented by the use of 5G worldwide?

Any U.S. networks operating internationally will inherently be required to operate with networks of unknown cybersecurity risk. The loss of information while operating on these networks would be detrimental to both the economic and security of the U.S. An architecture that

assumes all networks are inherently not secure is needed to protect the network from data loss and cyber intrusions.

(3) How should the U.S. Government best promote 5G vendor diversity and foster market competition?

As networks operate both domestically and internationally, there is always a risk companies will lose intellectual property ("IP") due to bad actors. Protection of IP is a key driver for vendors operating internationally. The U.S. Government should (1) advocate for aggressive protection of U.S. technology IP rights and (2) promote domestic innovation by fostering private enterprise IP.

(4) 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?

The U.S. has the ability to lead international 5G (or xG) in several ways. Two of the strongest areas are cyber secure systems and networks operating in FR2 (6 GHz+). The commercial ecosystems has significant capability in both areas. For 5G, these are emerging technologies. The U.S. can support growth in these areas by:

- Creating an emerging technology roadmap that includes, as a minimum, artificial intelligence, next generation Internet of Things (IoT) devices, cloud cybersecurity services, and machine-to-machine connectivity;
- Supporting open systems and open architectures; and
- Providing a way to evaluate developments in these areas with multiple vendors.

IV. 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?

The U.S. has the ability to lead international 5G (or xG) in several ways. Two of the strongest areas are cyber secure systems and networks operating in FR2 (6 GHz+). The commercial ecosystems has significant capability in both areas. For 5G, these remain emerging technology areas. The U.S. can support international growth in these areas by:

- Creating an emerging technology roadmap to address the U.S. 5G commercial ecosystem and its expansion to support international developments. This roadmap, as a minimum, should include artificial intelligence, next generation Internet of Things (IoT) devices, cloud cybersecurity services, machine-to-machine connectivity, both connected and disconnected peer to peer communications;
- Supporting open systems and open architectures;
- Providing a mechanism to evaluate, with multiple vendors, developments in these areas;
- Ensuring protection of international IP rights;
- Establishing R&D funding sources for early-stage emerging technologies, that show promise to solve critical issues as they arise; and
- Promulgating U.S. positions on standards and supporting international standards bodies for 5G and follow-on.

(2) How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies?

As a minimum, representatives from private companies, academia, public trust organizations, and the U.S. Government must work together to support international standards

developments. In this regard, the U.S. Government should exercise leadership in setting global norms and advancing U.S. interests. Academia brings thought leadership. Federally funded research and development centers and university affiliated research centers provide an unbiased approach to standards developments. Private companies provide the mechanism to ensure these standards meet their needs, are economically viable, and ensure the proper implementation timing is considered. Bringing these representatives together to work cohesively in a single direction is not a trivial endeavor. The U.S. Government should consider early sponsorship, including funding, of representatives to participate in standards discussion and committees.

(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?

5G provides more bandwidth, much higher densities of devices, and very low latencies over any previous network. As infrastructures deploy and systems take advantage of these new tools, it opens doors to exploitation within any infrastructure. It is not simply that security loopholes may exist within the infrastructure, it is also about which systems are allowed to host on the infrastructure. A better understanding of the risk for companies or individuals is the need to first trust the infrastructure and then establish mechanisms to ensure malicious hosted systems do not compromise their information.

This response addresses the initial key element, which is whether the infrastructure developer or component developers for the infrastructure be trusted to stop the infrastructure from being exploited. A start at building trust across multiple infrastructures is the use of open systems, both hardware and software. While this does not stop malicious actors directly, it does provide insight into the infrastructure allowing visibility where these actors can exploit private information.

The U.S. Government should lead an approach to use open systems across all deploying 5G and future infrastructures. As discussed in Question 2 above, representatives from private companies, academia, public trust organizations, and the U.S. Government should work together to support international open system/open source requirements.

(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?

Trusted network infrastructure is a fundamental key to promote secure global 5G deployment. The U.S. Government should work with our international partners and allies to establish competitive procurements for open systems infrastructures. Within the U.S., evaluations of open systems infrastructures is crucial. Sponsoring private industry to establish open infrastructure prototypes allows evaluation of the infrastructures using organizations with an unbiased approach. These can leverage the innovation centers or model cities previously discussed with participation from both U.S. and international companies.

(5) 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?

Supply chain networks for information and communications technology equipment and software need to reach beyond the primary acquirer, and should ensure third-party suppliers are meeting secure 5G requirements. Infrastructure developers, maintainers, and acquirers will benefit from a standardized means for conveying and tracking information about common issues related to both the hardware and software components across the supply chain. For 5G, the network is moving to a software-focused network and many hardware components are now virtualized in software. Hardware tools such as bill of materials for hardware transparency need to adapt to provide the equivalent for software. NTIA is currently working to develop the

equivalent in software transparency[4] that will be needed for secure 5G supply chains. Block chain used to ensure counterfeit or noncompliant hardware parts do not infiltrate the supply chain can also benefit software developments. Many software developers cascade components to form applications. End-to-end visibility across the supply chain and multiple enterprises is needed to ensure these components are traceable to a valid developer.

(6) What other actions should the U.S. Government take to fulfill the policy goals outlined in the Act and the Strategy?

For international infrastructure, supply chain integrity is critical to ensure there is an unbroken custody of material and software from sourcing to deployment. This ensures trust for infrastructure. The U.S. Government should work with our international partners and allies to ensure a common understanding of supply chain integrity across the international 5G commercial ecosystem.

V. CONCLUSION.

Raytheon supports the development of an implementation plan for the National Strategy to Secure 5G, and encourages the NTIA to incorporate the recommendations set forth above.

[4] https://www.ntia.doc.gov/SoftwareTransparency.

Respectfully submitted,

/s/ Michael L. Robinson
Michael L. Robinson
Director, Advanced Programs
mlrobinson@rtx.com

/s/ Sai Kalyanaraman
Sai Kalyanaraman, Ph.D.
Technical Fellow
sai.kalyanaraman@collins.com

/s/ Thomas A. Voltero, Jr.
Thomas A. Voltero, Jr.
Senior Counsel

Raytheon Technologies Corporation
870 Winter Street
Waltham, MA 02451

June 23, 2020