19 June 2020

National Strategy to Secure 5G

Docket No. 200521-0144

RIN: 0660-XC047

Cubic | Nuvotronics Response

Prepared for:

Department of Commerce
National Telecommunications and Information Administration
1401 Constitution Avenue, NW, Room 4725,
Washington, DC 20230

secure5G@ntia.gov

Prepared by:

Cubic | Nuvotronics
2305 Presidential Dr
Durham, NC 27703

Martin Amen
Vice President and General Manager (GM)
407.491.9815 | martin.amen@cubic.com

CUBIC™

NUVOTRONICS

1 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)?

A good example of how the U.S. Government can best facilitate the domestic rollout of 5th Generation (5G) technologies and the development of a robust, domestic, 5G commercial ecosystem is by investing in the deployment of the Cubic | Nuvotronics commercial 5G offerings. With Nokia Corporation (Nokia) that provides key technology to build a U.S.-manufactured capability, our Cubic/Nokia 5G Tech Bundle could be deployed to provide national 5G coverage with a clear path to Next-Generation (Next-G) capability. Rather than allowing uninformed discussion about how Huawei Technologies Co., Ltd. (Huawei), has the only viable 5G solution, the Government should recognize that the U.S.-based manufacturing line for the Cubic/Nokia 5G Tech Bundle could begin ramping up immediately upon receipt of a modest Nonrecurring Engineering (NRE) investment, and begin delivering units for commercial deployment by First Quarter (Q1) 2021. Cubic | Nuvotronics has all the necessary relationships with equipment manufacturers, chip manufacturers, software developers, cloud providers, system integrators, and network providers to help America's telecommunications providers rapidly deploy national-scale 5G coverage.

Considerations:

- Specify purchasing with 5G solutions and security.
- Create research initiatives in the area for non-typical DoD vendors.
- Consider creating trusted fabrication for "silicon" ecosystems for U.S. Government consumers.
- Create a unique 5G "govcloud" offering for needed services and security.
- Develop and specify 5G unique Peer-to-Peer (P2P) requirements and offerings.
- Resolve spectrum ambiguities globally and quickly, particularly greater than 6 GHz.
- Establish clear Artificial Intelligence/Machine Learning (AI/ML) linkage and oversight around 5G internally.
- Resolve its own Internet Protocol version 4 (IPv6) policies and execute a coherent strategy as a part of the 5G initiative.
- Consider 5G incorporation into National Intelligence Priorities Framework (NIPF) to focus intelligence on it.

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

If the Government's goal is speed, in terms of time to installation of a nation-wide 5G infrastructure, the current rollout of the various base implementation is an excellent approach. The Government should look to the various prototype proposals for enhanced solutions that foster U.S. innovation and manufacturing capabilities.

Considerations:

- Collaboratively consolidate research initiatives across DARPA, Intelligence Advanced Research Projects Activity (IARPA), National Laboratories, Service Laboratories, Federally Funded Research and Development Centers/University Affiliated Research Centers (FFRDCs/UARCs) for focus and impact.
- Distinguish between Test and Evaluation (T&E) and research activities. They are convoluted now.
- Consolidate test beds where possible and externalize their use.
- Establish agency primacy across Intelligence, Defense, and Civilian for 5G strategy.
- Engage Service Providers' (AT&T, VZW, etc.) research organization directly.

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?*

A key factor to further motivate the domestic-based 5G commercial ecosystem to increase 5G research, development, and testing would be to invest in innovative manufacturing capabilities that advance the United States. For example, Cubic | Nuvotronics has an additive manufacturing capacity that can produce technology far better than some adversary countries, no matter how difficult it may be to compete due to domestic costs as compared with adversary countries that have significant government investment. This could be accomplished through the Defense Production Act, Title III, which would enable the Government to rapidly invest in innovating manufacturing technology that can compete commercially and also provide military options at a desired economical state. In addition, broader prototype efforts and Research Development Test & Evaluation (RDT&E) investments could be made to develop Next-G chipsets, etc., to allow Cubic | Nuvotronics's innovative manufacturing process to go beyond 5G capabilities to address mobile communications, Internet of Things (IoT), and Next-G autonomous solutions.

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 U.S. Government should, for example, invest in rollout of U.S.-based 5G infrastructure such as Cubic | Nuvotronics's 5G dual-band transceivers with an applied RDT&E effort (biased toward development, testing, and evaluation). Cubic | Nuvotronics, as a private sector company, has already invested in 5G technology and beyond. The U.S. Government can engage with Cubic | Nuvotronics immediately to deploy 5G, and to engage on how to take full advantage of the Next-G capabilities we have to offer.

Considerations:

- Border Gateway Protocol (BGP)/Multiprotocol Label Switching (MPLS) (BGP/MPLS and backbone security ramifications)
- Radio Access Network (RAN), RAN, Radio Access Technology (RAT), Software-Defined Networking (SDN), and Network Function Virtualization (NFV) layer vulnerabilities and protections
- >6 GHz waveform handling, including in space
- High-density connection management

- Small cell and enterprise concentration management impacts
- Edge AI/ML implications, applications, and opportunities
- Creating a secure Next-G packet core – "the evolved packet core"
- Exploring convergence with 802.11 over time

2 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?

Even if the U.S.-manufactured Cubic 5G infrastructure solution is put into place across the United States, and as part of the U.S. expeditionary national security communications infrastructure, we must always assume a near-peer foreign adversary has compromised the solution. This core security principle is at the center of the secure channel encryption solutions that Cubic has provided to the Department of Defense (DoD) for many years, up to and including Type-1 National Security Administration (NSA) encrypted channels. Security principles must be established to determine which (if not all) telecommunications traffic should be secured from compromise through such approaches.

Direct security concerns include:

- Implications of the broadened attack surface of Radio Access Network (RAN), Software-Defined Networking (SDN), Network Function Virtualization (NFV), etc.
- Implications of insecure Border Gateway Protocol (BGP)/Multiprotocol Label Switching (MPLS) implementation/issues
- Virtualization insecurities, including Hypervisor concerns
- Application Program Interface (API) Security concerns and mitigations
- Micro-segmentation approaches to security and service delivery
- Cryptographic key management and synchronization
- Domain Name Service (DNS) evolution and hardening
- Security Function Virtualization implications
- Consider orchestration as a potential attack surface
- Multi-domain security operations
- New denial of service modalities
- Insider boundaries erasure implications
- Adversarial Machine Learning/Artificial Intelligence (ML/AI)
- Spectrum misuse
- Usage of Peer-to-Peer (P2P) models to improve security, reducing Man-in-the-Middle (MITM) attack surface

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 U.S. Government should consider looking beyond the traditional telecommunications equipment providers to a company that has security in its DNA, and that has experience providing solutions that secure our nation against peer and near-peer adversaries.

Considerations:

- Verifiable code provenance and Bill of Materials (BOMs)
- Supply chain interrogation
- Penetration testing
- Self-protection mechanisms
- A secure virtualized packet core
- The role of AI/ML and adversarial learning detection/prevention particularly in orchestration and virtualization
- Silicon and related hardware trustworthiness
- Source code validation testing to prevent remote hacking

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?*

Considerations:

- Protect, detect, and defend positionally in this currently "complicated" architecture and a simplified future state
- Self-securing services and infrastructure
- SFV as a standard
- Verifiability of trust

4) *Are there stakeholder-driven approaches that the U.S. Government should consider promoting adoption of policies, requirements, guidelines, and procurement strategies necessary to establish secure, effective, and reliable 5G infrastructure?*

There are existing contracts in place—that are only an MPIR away—that could be used for immediate procurement of 5G pilots, demonstrations, and deployments based on Cubic | Nuvotronics's technology offerings.

- Help drive and develop a 5G ecosystem.
- Provide Cooperative Research and Development Agreements (CRADAs) for innovation.

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?*

The Government should consider the following:

- Cooperative research programs
- Full-spectrum asymmetric approaches

3 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?

There are opportunities to extend the reach of U.S. international development investments to help finance developing nations' acquisition and implementation. For example, the Cubic/Nokia Tech Bundle offered under the 5G prototype demonstrates one way to expand a U.S.-based 5G capability globally.

Considerations:

- Market expansion
- Innovation through technology initiatives

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

There are opportunities to extend the reach of U.S. international development investments to help finance developing nations' acquisition and implementation of the Cubic/Nokia Tech Bundle. Market expansion and targeted innovation through technology initiatives extend the opportunity set and create new opportunities as other nations aggressively pursue their own foreign policy.

Considerations:

- U.S. Government ecosystem
- Competitive vis-a-vie China, etc. – Buy indigenous solutions campaign
- Tariffs, Buy American, and even sanctions

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

The U.S. Government should promote 5G vendor diversity and foster market competition by immediately investing in the Cubic/Nokia Tech Bundle, including RDT&E and city-wide pilots to de-risk acquisition in the face of Huawei's existing product offering. In addition, the U.S. Government should raise awareness of this U.S.-led commercial 5G capability in the conduct of its foreign policy and trade negotiations the same way that it advocates for Boeing airframes. Any new U.S. equipment vendor that offers similar capabilities could/should be added to this list for U.S. Government RDT&E investment and foreign trade policy advocacy.

Considerations:

- Offer Small Business Administration (SBA) type incentives.
- Help foster 5G start-ups.
- Provide CRADAs.
- Promote pan-geographical partnerships and innovation.
- Provide corporate tax credits for domestic manufacturers that can develop secure 5G products and can be trusted by any U.S. Government agency.

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?

Beyond deploying a secure 5G network infrastructure with the Cubic/Nokia Tech Bundle, it is essential that U.S. Government investment encourage U.S.-based, trusted foundry capabilities for creating competitively priced, trusted hardware solutions for mobile handsets, the Internet of Things, and more, that avoid zero day exploits inserted by foreign adversaries.

Considerations:

- Competitive vis-a-vis China, etc. – Enforce embargoed companies and non-U.S. origin enterprise policies and statutes.
- Mandate that domestic 5G manufacturers adhere to specific security enabled standards.

4 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. Government, for example, can lead international development with joint agreement with friendly European partners that do not just focus on the United States, but globally, where the European markets are established.

Considerations:

- Start-up innovation incentives.
- Competitive vis-a-vis China, etc.
- Create cross-border collaborative partnerships.
- Handle Counterintelligence (CI) and Foreign Ownership, Control, or Influence (FOCI) issues clearly and consistently.
- Create an international 5G consortium that will police the practices of all 5G manufactures and report results quarterly to industry.

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

The U.S. private sector already participates in standards development for 5G technologies, but the U.S. Government abandoned its commitment long ago to U.S.-based manufacturing of these technologies. The Government must fund U.S. manufacturers of 5G technologies immediately, and work with them to shape the Next-G standards by forging the frontiers of new, cutting-edge, scalable, secure, and commercially viable product offerings.

Considerations:

- Provide leadership through focus.
- Approach indigenous visionaries to participate.

- Create an annual 5G developers conference and allows industry to present white papers and potential prototype products.

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?*

With Cubic | Nuvotronics, the U.S. Government has at its disposal a U.S. manufacturer with game-changing 5G technologies that could fundamentally transform U.S. telecommunications over a handful of years. The approach would be to fund the activities discussed above, immediately, and to begin ramping up massive U.S.-based manufacturing of these 5G technologies for national and global scale deployment.

Considerations:

- Provide Security assessments.
- Understand and protect backbone infrastructure security risks and exposures
- Plan and provide war game catastrophic network calamities for defense and recovery.
- Create specific security protocols and standards for U.S. Government entities that wish to access 5G networks in an Outside the Continental United States (OCONUS) environment.

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?*

To promote, foster, and encourage international cooperation around secure and trusted 5G infrastructure, the U.S. Government should provide technical exchanges, flying in telecom engineers from around the world to train on the U.S.-based solution sets. This should be treated as public diplomacy, including international networking opportunities as well as continuing learning credits.

Considerations:

- Provide collaborative test environments.
- Offer Joint exercises with allies.
- Plan and provide war game catastrophic network calamities.
- Provide tax incentives to U.S.-based 5G developers that create and enforce specific standards that their international partners must abide by.

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.4 Are there other models that identify and manage risks that might be valuable to consider?*

We suggest a model that issues rules forbidding the purchase and deployment of Huawei hardware in the telecommunications infrastructure supply chain, or a "buy American" rule. The Government promulgation of complicated security monitoring standards for the commercial telecommunications companies would never keep up with the fast-changing technology space. A U.S.-based industry association could establish standards, but it is unclear how they would actively identify and manage risks experienced by telecom operators. A private sector, third-party, security-monitoring framework would require invasive access of one commercial

organization into the technical infrastructure of another, creating all sorts of problems. A public-sector-based, security-monitoring framework for managing risks would require Government (Department of Homeland Security/National Security Agency [DHS/NSA]) monitoring of domestic communications infrastructure, which would be politically untenable.

Considerations:

- Use spectrum as a national asset.
- Conduct regular risk identification, management. and mitigation exercises.

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

The U.S. Government should stop saying that there is no U.S.-led 5G manufacturing capability and take a small portion of the resources that have been appropriated in Fiscal Year (FY)20 to accelerate the Cubic/Nokia Tech Bundle as part of the broader 5G prototype efforts into large-scale manufacturing and deployment.

Considerations:

- Lean in on AI/ML integration.
- Offer competitive positioning visa-vie China etc.
- Define the security standards required for domestic 5G Original Equipment Manufacturers (OEM).

ACRONYMS

Acronym	Definition
5G	5th Generation
AI	Artificial Intelligence
API	Application Program Interface
BGP	Border Gateway Protocol
BOM	Bill of Materials
CI	Counterintelligence
CRADA	Cooperative Research and Development Agreement
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DNS	Domain Name Service
DoD	Department of Defense
FCC	Federal Communications Commission
FFRDC	Federally Funded Research and Development Center
FOCI	Foreign Ownership, Control, or Influence
FY	Fiscal Year
Huawei	Huawei Technologies Co., Ltd.
IARPA	Intelligence Advanced Research Projects Activity
IoT	Internet of Things
IP	Internet Protocol
MITM	Man-in-the-Middle
ML	Machine Learning
MPLS	Multiprotocol Label Switching
Next-G	Next-Generation
NFV	Network Function Virtualization
NIPF	National Intelligence Priorities Framework
NRE	Nonrecurring Engineering
NSA	National Security Administration
OCONUS	Outside the Continental United States
OEM	Original Equipment Manufacturers
P2P	Peer-to-Peer
Q1	First Quarter
RAN	Radio Access Network
RAT	Radio Access Technology
RDT&E	Research Development Test & Evaluation
SBA	Small Business Administration

Acronym	Definition
SDN	Software-Defined Networking
T&E	Test and Evaluation
UARC	University Affiliated Research Center
U.S.	United States