Commonwealth Cyber Initiative

900 N Glebe Rd., 3rd Floor
Arlington, VA 22203

Response to request for comments to inform the National Strategy to Secure 5G Implementation Plan (Docket No. 200521-0144)

Submitted by

Prof. Luiz DaSilva, PhD
Executive Director, Commonwealth Cyber Initiative
Bradley Professor of Cybersecurity, Virginia Tech

On behalf of the

Commonwealth Cyber Initiative (CCI)

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)?

- Develop a clear country-wide 5G strategy, supported by specific research and innovation programs designed to regain the leadership in 5G commercial R&D and establish leadership in 6G research and standardization efforts.
- Emphasize the need for “security-by-design” that touches the entire supply chain.
- Make more spectrum available for commercial use, including spectrum needed for wireless backhauls that are likely to be deployed in remote/rural locations.
- Streamline the federal/state/local governments’ rules and regulations for approving 5G infrastructure deployment.
- Identify key domestic stakeholders and international partners for developing security principles for 5G/6G infrastructure and ecosystem.

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

- Leverage U.S. universities to create disruptive technologies that go beyond the 3GPP releases associated with 5G.
- Establish programs in NSF specifically targeting basic research on the development of technologies for 5G and beyond, coupled with experimentation at scale in testbeds.
- Expand DARPA and DoD programs targeting the development, deployment and adaptation of 5G for military use.
- Create sponsored programs and/or centers that encourage and incentivize joint academic and industry R&D in 5G and beyond, and incentivize the translation of basic research into innovation.

- Include 5G considerations in the strategic planning for future initiatives in manufacturing, transportation, energy, and other verticals.
- Support the development of new benchmarking and testbed facilities targeting 5G and beyond.
- Establish a 5G Range that provides the ability to evaluate 5G technologies by stakeholders in autonomy, IoT, AI, and other 5G enabled use cases.
- Develop a 5G cyber risk assessment capability similar to NIST's National Vulnerabilities Database that would provide deeper insight into security readiness of 5G software and hardware.

(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?

- Organize a national dialog between academia, private sector, government, around the country's priorities in 5G and beyond. Universities can play an important role as a convener that gives arms-length to government involvement.
- Support the participation of domestic industry representatives and researchers in standardization bodies, representing a common national agenda on 5G security.

(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.

- Focus on the areas of promise for 5G and edge computing where the main opportunities for innovation lie: provisioning of reliable communications for a new generation of applications, from autonomous vehicles to widespread augmented reality, from industrial automation to the tactile Internet.
- Invest in the softwarization trends in 5G (e.g., software-defined handsets and networks, network function virtualization, cloud computing), and open radio access network efforts.
- Promote spectrum sharing, including license-exempt access to certain bands to accelerate innovation.
- Investigate the use of artificial intelligence (AI) to create more robust networks that are easier to deploy.
- Develop automated tools to check for security vulnerabilities.
- Develop war-gaming approaches to validating security and for checking on vulnerabilities, especially from a high-level network perspective.

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?

- Potential for widespread international adoption by governments and standardization bodies.
- Coordination with similar efforts initiated by the governments of U.S. allies; for example, the EU toolbox of risk mitigating measures.
- Selection of metrics and development of open benchmarks.
- Validation and certification of products as meeting the security principles.

- Emphasizing “security-by-design” for all 5G software and hardware.
- Developing more sophisticated and automated testing techniques to locate security vulnerabilities.

(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?

- Validated testing scenarios, experimented with at scale, under simulated attacks.
- Shared accountability in 5G supply chain between suppliers, vendors and users.
- Increased transparency and access to information pertaining to security threats plaguing 5G infrastructure to industry stakeholders, which can be addressed through the creation of a vulnerability database.
- Support for the development of formal and semi-formal tools for 5G verification.
- One key gap is in the development of methods to determine when a connection is being monitored, not just disrupted.

(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?

.

- Develop quantifiable risk and resilience metrics, coupled with a security auditing technique.
- Provide the ability to track the metrics through a 5G cyber security focused Information Sharing and Analysis Organization (ISAO).
- Proper delineation of the requirements abstract vs. system-level requirements so that the “shall”s can be directly traced to the mechanisms implementing them, and so that non-implementable requirements can be identified.
- Security requirements should be checked for completeness and consistency, and formal or semi-formal representations should be checkable by automated means.

(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?

- Developing a U.S. version of the toolbox of risk mitigation measures, arrived at by consensus between government, industry, and academic research participants.
- Coordinated representation of U.S. interests in international standards bodies involved in the evolution of 5G.

(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?

- Easy access to license-free or lightly licensed spectrum to incentivize innovation.
- Incentives for shared accountability in supply chain that results in access to trustworthy hardware and software.

- Investigation of new business models that incentivize manufacturers and operators that meet security benchmarks.

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?

- Innovation and start-up creation in a new generation of applications and services, enabled through the low latency, reliability, high data rates, scalability brought about by 5G.
- The U.S. is strong in software and application development, areas that are, in many ways, more profitable than 5G hardware. As these apps are developed, helping to facilitate best practices in security can help. To some extent, security concerns can be addressed at the application level.
- Establishing leadership in Beyond 5G/6G.
- Expansion of export markets for 5G-related U.S. industries.

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

- Broad awareness that vulnerabilities of 5G infrastructure worldwide present risks to national security. This goes beyond just nation-state threats but also covers terrorism and natural disasters.
- Unavoidable use of non-U.S. software/hardware of questionable trustworthiness in the U.S.'s 5G infrastructure (due to unavailability of software/hardware produced by U.S. industry) requires systematic risk analysis of 5G infrastructure and the evaluation of degrees of confidence in the supply chain.

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

- Provide preferential access to U.S. companies to intellectual property generated by US universities under a federal contract.
- Fund R&D in standards-compliant network stacks for 5G as well as beyond 5G that are open source by design. This will encourage the decoupling of the software and hardware ecosystems of 5G. This, in turn, will mitigate the threat posed by supply-chain attacks and promote 5G vendor diversification and market competition.
- Provide seed funding for innovation, especially for startups and SMEs.

(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?

- Workforce training program in 5G, including both the telecommunications/software engineering workforce and workforce involved in R&D in key verticals. This is particularly important in verticals that have high potential to be revolutionized by 5G, such as smart transportation, advanced manufacturing, and healthcare.

- Programs to attract and retain top international talent.

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?

- Funding programs that support international collaboration, partnerships with countries in Europe, Asia, and the Americas for joint academic and research programs around 5G.
- Promoting and funding participation in standards bodies responsible for 5G and related technologies.
- Develop de facto standards and promote best practices for 5G security implementation and 5G secure supply chains that other countries may be able to adopt.

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

- Organizing a recurring national dialog between academia, private sector, government, around the country's priorities in 5G and beyond, and promoting and funding the representation of national priorities in the 3GPP standards process. Universities can play a key role as conveners.

(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?

- Blockchain-empowered information sharing that will provide provenance for vendors' and suppliers' actions.
- Develop and employ vulnerability testing software.
- Work with allies and international partners to develop cyber risk-management policies for 5G systems.

(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?

- Establish partnerships with research funding agencies in Europe, e.g., as part of the upcoming Horizon Europe program, and selected countries in Asia to enable funding for international cooperation in 5G and beyond research.
- Fund universities to engage with exchange programs with leading universities in Korea and Europe that are considered international leaders.

(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?

- One might consider a “UL” (Underwriters Lab) model for security. That is an independent lab that performs a security analysis of the software and certifies this software.

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

- We need to be thinking about how to harden the infrastructure so that if certain elements of the infrastructure are compromised or destroyed, that we have backup systems to circumvent this loss.