Booz | Allen | Hamilton®

The National Strategy to Secure 5G

NTIA REQUEST FOR COMMENTS, JUNE 2020

Prepared for National Telecommunications and Information Administration (NTIA)

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

TABLE OF CONTENTS

1 COMMENTS ON NTIA 5G NATIONAL STRATEGY

This report provides Booz Allen's response to the NTIA's 5G request for comments on the Implementation Plan for the National Strategy to Secure 5G. It addresses the NTIA's questions for lines of effort one, two, and four from the Federal Register Notice Vol. 85, No. 103.[1]

1.1 Line of Effort One: Facilitate Domestic 5G Rollout

1.1.1 5G DOMESTIC ROLLOUT

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)?

Without direct U.S. investment, the U.S. could fall behind in the development and production of 5G technologies, which could hinder our competitiveness and the security of our networks. Both U.S. investment and infrastructure actions can improve this position and domestic rollout.

Investment is needed in each area of commercial 5G to stimulate the ecosystem, and especially in areas where the U.S. has divested capability and talent overseas (e.g., in semiconductor fabrication). We need to prioritize investment to directly address the areas where we fall short in international competition. While the private sector plays a role in investment in 5G, from a public sector perspective the U.S. Government research and development (R&D) spending (e.g., from Defense Advanced Research Projects Agency (DARPA), Intelligence Advanced Research Projects Activity (IARPA), National Science Foundation (NSF), National Institutes of Standards and Technology (NIST), Department of Transportation (DOT), or related groups) can help prioritize and fund related investments. Investments made must also be scaled to match the size of the challenge and delivered quickly to have impact.

Infrastructure can also facilitate domestic 5G rollout. 5G is not a stand-alone capability, nor is the internet. The internet relies on governance, undersea cables, fiber infrastructure, and precise timing. None of this infrastructure is provided by the majority of the ecosystem, and it is often unknown to the users. The following steps can help in further addressing infrastructure for 5G:

- The U.S. needs to take on a leadership role in 5G standards and governance. From a public sector perspective, multiple federal agencies including the Department of Defense (DoD), DOT, Department of Homeland Security (DHS), and others have a stake in the use and standards for 5G. Currently there is a fragmented approach across the commercial and public sector (comprised of DHS, NSA, etc), resulting in stove pipe approaches and insufficient collaboration. Taking this leadership role may necessitate creation of an incentive system for U.S. companies and subject matter experts to contribute to the development of standards.

[1] Reference: Federal Register, Vol. 85, No. 103, Thursday, May 28, 2020, https://www.ntia.doc.gov/federal-register-notice/2020/request-comments-national-strategy-secure-5g-implementation-plan

- The DoD, DOT, and NIST should establish a national timing system to provide precise time to the 5G stations, which will be in greater number and densities than current 4G and earlier nodes. Timing through physical connections or Global Positioning System (GPS) (requiring rooftop leasing and antennas) is a multiplicative cost to the infrastructure providers. These costs will likely increase as 5G nodes become more dense and are deployed inside structures such as malls and office buildings. A system like enhanced long-range navigation (eLORAN), envisioned by the National Timing Security Act of 2018, could address this challenge and greatly reduce the infrastructure costs. It could also prevent the procurement of millions of dollars of timing infrastructure by the providers.
- Spectrum is a limited and contested resource. Spectrum (re)optimization is needed to promote (a) sufficiency and (b) diversity. The Ligado (formerly known as LightSquared) situation highlights the challenges of spectrum allocation, as does the DoD reluctance to release certain frequencies for 5G use. Lead spectrum organizations such as the NTIA, Federal Communications Commission (FCC), and other federal agencies and departments must take a holistic approach to assessing how best to adapt and reset spectrum allocation across the U.S. and with international partners.

1.1.2 PROMOTION OF RESEARCH, DEVELOPMENT, TESTING, AND EVALUATION

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

Without a focused R&D effort, the U.S. may not have the leadership position it could otherwise attain on 5G. The US needs enhanced collaboration between the NIST, National Security Agency (NSA)/Central Security Service (CSS), DARPA, and IARPA, to collaborate on R&D. This group can also develop standards with a U.S.-based center to provide test beds, instrumentation, security testing, and prototyping.

DoD, NSF, NTIA or another agency could establish a grant system to focus and drive success through academia. This would help to focus U.S. universities on 5G issues critical to the U.S. and provide a work force base that may want to continue working to support 5G in private industry, the Defense Industrial Base (DIB), or the Federal Government after graduation.

1.1.3 MOTIVATING DOMESTIC-BASED 5G ECOSYSTEM

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

Research and development is critical to leadership in 5G and beyond technologies. If such R&D is not motivated or encouraged, the U.S. risks its leadership in cellular wireless technologies. To address this issue, the U.S. Government can take the following steps to motivate the U.S. 5G ecosystem:

- Supporting timing systems to enable broader time division duplex (TDD) deployments without over reliance on GPS or significant capital infrastructure investment. This can be achieved through DoD/DOT/DHS leadership in timing system development and through general support for the development of such systems.
- Continuing support of spectrum modernization / shared approaches to spectrum licensing. The challenges and operating characteristics of available spectrum bandwidth can impact system design and architecture. Efforts led by FCC and NTIA can coordinate this with multi-year plans and roadmaps that are coordinated with other federal government departments and agencies.

- Designating a lead agency/office in the White House like the Office of Science and Technology Policy (OSTP) or a newly created office to build a federal portfolio around 5G like we did for nanotechnology. This investment portfolio could include leads from different agencies to coordinate investment in the following areas to galvanize US industry: U.S. Department of Health and Human Services, Department of Transportation (autonomous vehicles), Department of Housing and Urban Development (HUD) (smart cities), Customs and Border Protection (CBP) (Smart Borders), Department of Education (Smart Schools), DoD, the Office of the Director of National Intelligence (ODNI), Department of Commerce, Department of Agriculture, and others as applicable. Each of the agencies could fund a variety of pilots to demonstrate the application of 5G and related technologies to specific mission areas or Department priorities.

1.1.4 RESEARCH AND DEVELOPMENT PRIORITIES

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.

Without targeted and planned investment, the U.S. may fall behind foreign-based companies and initiatives in developing and leading 5G technology. There are several areas where the U.S. government should incentivize research and development. This R&D can be conducted by federal departments and agencies including DoD, DHS, and DOT. The following is a list of research areas to spur further development:

- Spectrum innovation (e.g., dynamic spectrum sharing and access)
- Novel applications and new use cases that take advantage innovations in 5G and future generation technologies
- Infrastructure innovation (e.g., leveraging low earth orbit (LEO) space (orbiting data nodes) and a national timing system)
- Intelligent data mining on the fly
- Security innovation (e.g., zero trust in a dynamically connected environment)

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

1.2.1 FACTORS FOR CORE SECURITY PRINCIPLES

What factors should the U.S. Government consider in the development of core security principles for 5G infrastructure?

Security for the 5G ecosystem should cover existing cybersecurity practices, but also needs to address the novel applications, devices, and infrastructure that 5G introduces. To do this, efforts need to consider the core premises of 5G, which are the increased fidelity and mobility of data. Each U.S. Government agency or department using 5G should consider the related security challenges, which include:

- Ensuring privacy

- Ensuring integrity and security of data

- Ensuring robustness of decision techniques and dependencies
- Ensuring the ability to detect and defend
- Ensuring system resilience (given dependencies and complexities of infrastructure). National timing infrastructure provides resilience of accurate timing
- Ensuring end-to-end security including the end points. 5G is an enabler of edge computing, which is going to increase the attack surface.

U.S. Government entities should consider and leverage the prior security research performed for Long Term Evolution (LTE) and 5G systems. For example, in security analysis done on L1 and L2 of LTE, studies show physical and link layer vulnerabilities that exist now in LTE and will likely continue in 5G if the same underlying waveform architecture is kept. Vulnerabilities could include identity mapping, using resource allocation monitoring as a side channel to perform activity fingerprinting, or integrity protection attacks on encrypted LTE user data.

1.2.2 FACTORS FOR EVALUATING SECURITY GAPS

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?

Software stacks derived from open-source code present in Original Equipment Manufacturer (OEM) software bases present unique supply chain and security challenges to 5G infrastructure. This software may be without specific origin but is key to network operation.

Users may be leveraging public 5G networks without high levels of computational trust. This results in a need for zero trust architectures and services for users to communicate securely over unsecured networks. Lead agencies such as NIST and DoD CIO can establish and maintain security architectures. Reference implementations could aid adoption of zero trust architecture. U.S. Government agencies and departments implementing 5G can build in security to their use cases and infrastructure by following these approaches.

1.2.3 USEFUL AND VERIFIABLE SECURITY CONTROL REGIME

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?

There are existing technical security standards for various parts of the 5G ecosystem; however, as 5G is being developed, not all security aspects have been analyzed. A security control regime that can be followed by the U.S. Government, its partners, and those in the community would aid the overall security posture for 5G networks.

A useful and verifiable security control regime would be one that is (A) automated and largely removed from user management/responsibility and (B) managed by existing cybersecurity services capable of handling cryptography and other security controls. This program could be established by NIST at a national level and work with federal department and agency security programs (e.g., NIST, DHS Cybersecurity and Infrastructure Security Agency (CISA) and Cyber Security Division (CSD)).

To increase availability of more security features in the 5G ecosystem, the Government could require security controls for networks where it is a user and thereby push the overall market to offer enhanced security features. This approach could be achieved via a FedRAMP-like entity to certify 5G networks for U.S. Government use. NIST's Computer Security Division (CSD) could establish a reference architecture including the security features to set standards for different components across the 5G ecosystem.

Certification frameworks or approaches to certify carrier networks and equipment for security compliance would aid the verification of this approach. Certification requirements for vendor products could further spur the market to implement secure 5G components and build secure 5G networks. This approach could be tailored with different levels of certification depending on the type of work to be performed.

FedRAMP could be expanded to multi-access edge computing environments that connect into a 5G network. The use of National Information Assurance Partnership (NIAP)-like certification approaches could be taken with the certification of 5G products.

1.2.4 PROMOTION OF ADOPTION OF POLICIES, REQUIREMENTS, GUIDELINES, AND PROCUREMENT STRATEGIES

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?

Delays or barriers to 5G implementation and adoption in the U.S. will negatively impact U.S. leadership in next generation wireless. U.S. Government departments and agencies with 5G use cases (e.g., DoD, DOT, DHS, HHS) can promote adoption through mechanisms including the following:

- Shaping the market using the Government's procurement power and lending credibility towards innovative approaches. Its procurement strategies could specify that network components and end-user devices can only be purchased if they meet certain security standards (e.g., NIST standard security controls).
- Engaging with industry groups for guidance on how to ensure security and supply chain security associated with 5G components. U.S. Government groups including ODNI and DoD Office of the Secretary of Defense (OSD) can lead industry interaction in this area.

1.2.5 INCENTIVES

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?

Without incentives for security, some 5G products and infrastructure components may be developed in an expedited fashion to meet financial goals and may not implement all security controls that the U.S. Government requires for its operations. As a buyer, the USG could incentivize contract award to companies that meet minimum security standards set by competitive industry standards and that meet federal guidelines. As part of this, the U.S. Government should leverage work from NIST cybersecurity division and national security requirements to create references and applicable standards for security in these solicitations. This will help to ensure security is considered and addresses security gaps in 5G infrastructure.

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

1.3.1 INTERNATIONAL DEVELOPMENT FOR SECURE AND RELIABLE 5G

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?

Secure and responsible use of 5G technology relies on secure sourcing and a secure supply chain approaches since the complete product supply chain can include untrusted parties. U.S. Government Supply Chain Risk Management (SCRM) efforts from DoD OSD, ODNI, and other groups can take several steps to address this challenge including:

- Encouraging expanded capacity to manufacture components domestically and develop firmware/software intellectual property (IP).
- Creating incentives to ensure security in the supply chain including for firmware, software, and semiconductors. Automation can be applied to ease the process of verification. For example, some semiconductor designers have robust anti-tamper evaluation for firmware and semiconductors to identify their IP in other products. This approach could be adapted to finding stray circuits and other nefarious components. This is an example of the type of tool that could be used to evaluate the supply chain risks associated with using specific 5G equipment and components.

Secure and reliable 5G is dependent on the standards and specifications used to build products across the 5G ecosystem. However, international development and deployment involves a variety of product vendors and parties each pursuing their own interests. To ensure the U.S. Government's interests are considered and that 5G technology can be appropriately used for U.S. Government use, the following considerations may be helpful:

- Engaging with national standards bodies to collaborate and draft security and reliability standards that can be baked into commercial products. The U.S. should increase engagement with national and international bodies to collaborate and draft security and reliability standards that can be built into commercial products.
- Encouraging mechanisms to validate the implementation of these national standards prior to procurement. To facilitate this, the U.S. Government needs to come in as a consumer by requiring security as part of a FedRAMP or NIAP-like program. This will help to drive investments in security and set the example for the rest of commercial industry.

1.3.2 FULFILLING POLICY GOALS

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

Over the past 5-10 years, U.S.-sponsored involvement in standards development organizations (SDO) has been low, and U.S. government sponsored analysis-driven contributions have been minimal. Engagement by other international and foreign-sponsored subject matter experts has pushed technical solutions. For example, in many of the 5G New Radio (NR) Radio Access Network (RAN) standards developed, People's Republic of China (PRC), China Mobile, Huawei, and ZTE all submitted independent (but relatively similar) proposals to the International Telecommunications Union (ITU).

These SDOs are contribution driven –when U.S. industry competes against a nationally sponsored interest to drive standards development, their investment tends to significantly outpace our own. If the U.S. subsidized industry (or even individual Subject Matter Expert (SME)) participation in these groups, the U.S. Government may see significantly more participation and input from U.S. companies in international standards. U.S. Government agencies and departments with 5G use cases, including DOT, HHS, Veterans Affairs (VA), DHS, DoD, and others should seek their own representation, incentive system, and contributions at these standards venues. The U.S. Government may consider establishing a federal working group to coordinate input and participation into standards groups.

In closing, Booz Allen appreciates the opportunity to provide comments to this Request. We believe it is vitally important to continue the advancement of technology through close collaboration with industry and government partners.

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.