SecureG, Inc
Response to NTIA Request for Comments
Docket No. 200521-0144

Development of an Implementation Plan for the National Strategy to Secure 5G

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 the domestic rollout of 5G technologies in ways that can also further the development of a 5G market ecosystem. As a critical early adopter of 5G, the U.S. Government is in a position to support 5G in several essential ways.

1. It can accelerate market demand to launch and sustain needed innovations by being one of the early adopters especially in critical mission areas such as within DoD and Public Safety.
2. It can also be instrumental in defining the necessary security requirements such as stating how it plans to implement a Zero Trust Architecture when using 5G mobile communications that will span across many domains of system ownership – where no one single entity is the provider of security situational awareness.
3. By defining operational requirements in reliability and latency, the U.S. Government can be a forerunner to test and find solutions to implementation challenges in the advanced 5G use cases that intersect with critical infrastructure.
4. This will mean investing in the prototypes, spending R&D dollars that can quickly find the best solutions and transition the winning prototypes into production.
5. The U.S. Government can also make clear its requirement for trust interoperability across the many to many domains in a 5G connection path. The Department of State Clean Path Request for Information is an example of these kinds of government requirements.

In all these examples, the government is acting within its mandate supporting its mission requirements but also for how the 5G technologies can serve private sector needs by creating the ecosystem of companies that will be the providers for the commercial sector demand as it grows.

There is no single U.S.-based and certainly no single global provider of the 5G communications connection path and no entity that can on its own provide path assurance awareness. The infrastructure must support the concept of ‘many to many’ - many kinds of devices, many enterprises, many radio bands, many carriers, and many cloud-provided applications. All of

these need to make 5G connections and interoperate at an incredible scale. Trust interoperability is required between different elements of the connection path for the static (non-mobile) and the dynamic (mobile and on-demand) platforms, between different system owners, roaming between different connection providers and trust interoperability crossing geographic boundaries.

The U.S. Government should be prescriptive about the security requirements of 5G systems that extend beyond the traditional Confidentiality, Integrity, and Availability (CIA). The past few months have made clear the tenuous nature of supply chain trust in a crisis. Privacy, Authenticity (a part of provenance), Device Authentication, and Availability as pertains the assurance that a service cannot be deliberately disrupted by the provider to protect system and data integrity need to become additional fundamental elements of defining trust in 5G systems. Implementors of CIA in 5G need to expand to include the elements of security described here. The U.S. Government can be a facilitator explaining why these additional elements are central to the cybersecurity protection requirements for all sixteen Department of Homeland Security Critical Infrastructure Sectors.

Through all of these technical challenges, the question of how to handle the establishment of trust is equally critical. It is a governance challenge that requires a governance framework including stakeholders at an international level. We must include the means to enforce those rules via solid governance that includes enforcement that polices itself in real-time. The U.S. Government should be a critical stakeholder in this process.

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

Innovation increases come when there is a known market need. As noted above, the U.S. Government can help drive innovation by being an early adopter in this space. It can encourage others into the market by helping define the security and operating requirements of the 5G network. All this must be done with the mindset of being one of a set of critical stakeholders representing the 5G future use cases from the designated sixteen critical infrastructures (CI). Defining these market needs in 5G will spur the innovation as the CI Sectors and the inventors work together to develop the 5G infrastructure and market.

Regarding actions that only the U.S. Government can take, the government needs to put aside a spectrum for development; call it the “Innovation Band” operating in both sub6 and millimeter wave It must be one good enough for testing, for R&D, for trying out new mesh architectures.

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?

The National Spectrum Consortium (NSC), a partner with the DoD, models the type of activities that the U.S. Government can take to motivate more commercial sector R&D. The NSC recently received Requests for Prototype Proposals (RPPs). The RPPs were structured in a three-phase delivery that in Phase Three would transition (if successful) to an Authority to Operate (ATO) request at production scale. Commercial industry sees this approach as one that recognizes that the 5G technology is at a prototype stage. Bidders to the RPP have the expectation that the innovations already started will be for prototypes with a specific use case such as smart warehouse operations. It also has the expectation that winning bids have an exit with the ATO where the government will be a buyer of the developed technology at production scale. These are the incentives that private sector investors look for – the motivation – as they see the development of a market that can then expand to the private sector.

This is a good model. Other parts of Government (e.g., Department of Commerce) could join it, no need to reinvent it, as a way for the U.S. Government to consider when planning how to further motivate domestic research, development, and testing of 5G. The DoD is leading because they have an expectation that 5G will meet mission requirements unmet today. They are not going to their traditional R&D route; rather, they went to industry for buy-in to the solution for the whole of the many industry sectors. This willingness to rely on industry is motivating to the investment community and innovators. They want work to proceed at an 'Internet pace' not traditional R&D pace.

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.

A critical area for priority is in 5G security. Security in IT systems engineering has traditionally been done as an afterthought and then done piecemeal. It has not been handled as part of holistic system approach that considers user, data, control, and management planes that need to be provisioned securely and operated securely. This approach is known to introduce expensive and difficult problems into a system, and yet it continues to be a common approach used when speed to market is the overriding objective. It is called bolt-on security. Developers and manufacturers know that there is an up-front cost to security in the development lifecycle but view the resource costs as too high. As a result, we see companies manufacture and deploy vulnerable technologies, passing the problem to the security practitioners left with the bolt-on approach as the only option, to buy another point solution of security technology (more security complexity) to offset the latest threat that we failed to anticipate.

Bolt-on security is a failed model; it won't work in the 5G, highly virtualized, highly distributed mobile, cloud-centric operations. In the new model, Zero Trust for 5G, it could solve problems

in existing bolt-on approaches considering how 5G's fundamentally new architecture can be used as a tool to combat cyber issues in ways that are not feasible in a legacy Internet architecture. Pervasive use of a Zero Trust approach for software defined networks (SDN) and Network Function Virtualization (NFV) could be used to block DDoS/botnet activity at the source or using network slices to move critical infrastructure of the public Internet.

The U.S. Government is rightfully concerned for the security of the 5G critical infrastructure. That concern now includes the possibility that the supply chain could be compromised with backdoor channels; the vital channels of communication could fail in a time of crisis between nations. They want it to "be secure" and require a change to a "Zero Trust Architecture" approach to security. However, the root causes, as described, will remain if not addressed directly. These concerns for the security of 5G infrastructure and the concepts of Zero Trust alone won't solve for the market factors, won't force a change to the absence of security practices in the engineering discipline, and won't force the market to develop the solutions for security as a holistic problem. Security designed in from the beginning, end to end, is the goal for the 5G infrastructure and it needs more than words and concepts. It needs standards and implementations.

Making statements that 5G must be secure and making Zero Trust requirements is a start, but it must further include the implementation requirements. The 3GPP R15 (and soon R16) is a beginning, answering part of the 'how' question with the use of cryptography, specifically the public key infrastructure (PKI) for present. It will require pioneering the move from classical cryptography to post quantum cryptographic (PQC) key material in PKI certificates, providing a secure transition from existing techniques to the Post Quantum era for its participants. PKI with PQC can enable a Zero Trust Architecture securing the 5G communications transactions.

Enabling a 5G Zero Trust Architecture will provide a way to consistently implement the Zero Trust requirements of authenticating and authorizing everything in the connection path between many domain owners. Zero Trust in mobile, cloud-centric systems must also operate in ways consistent with ultra-reliable, low-latency operational requirements that represent the advanced use cases that go beyond just faster broadband connections. It must work for the 5G Phase Two uses cases and scale to the massive machine type communications requirements of IoT and IIoT. The U.S. Government can be clear that it will be one of the first major market buyers of the 5G security-enabled solutions that can meet these requirements. The market of innovators is ready to deliver when these expectations are clear, and the market potential is there.

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?

The first critical factor for the U.S. Government to consider is the need for trust interoperability. A second critical factor is the need for connection path assurance as the basis for making trust decisions and to mitigate concerns about the integrity of supply chain.

There are many devices in the enterprise and many ways of radio access connecting to many means of mobile edge computing (MEC), or to the front-, mid-, and backhaul connections to the carrier 5G core. There may be many carriers involved in a roaming connection and there are definitely many cloud providers needed to provide data and applications. All these "many" types of domains, include the many types of equipment and software to make the connections, are generally provided as virtual functions. If Zero Trust is a requirement, and there are many owners in the connection path with many providers of the technology, then a way to have interoperable trust is a core security principle for the 5G infrastructure.

At present time there is no way for an enterprise to request and get assurance that the connection path for a critical communications slice is provided by known and trusted components, both physical and virtual. Path assurance is another principle for security in the 5G infrastructure for connections that require high levels of trust.

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 can be clear about the requirements for operating the 5G infrastructure in ways consistent with its obligations of national security. This can include principles of provenance—aligned to the Prague Proposals for 5G Security the ability to know the source and reputation of the technology providers in the infrastructure during installation and in operation—that will serve as the means to provide path assurance. It can also include a requirement for security testing at the component and system level, another critical factor to provide assurance that the U.S. 5G infrastructure operates in a manner consistent with expectations of security and privacy assurance.

The issue of provenance is a central element related to trustworthiness. It informs responses to the questions around the provenance of the device, the software code, and the overarching infrastructure. Questions such as: Where did the technology making up the infrastructure come from? What are the methods of control to assure that a foreign government cannot exercise its authority over a technology manufacturer to deny the use of that technology in a moment of crisis? The past few months make this question of establishing supply chain provenance one of the essential elements of determining trustworthiness.

The role for the U.S. Government is to help establish requirement that allow for making these kinds of different trust decisions in clear and transparent ways for the supply chain and how the equipment / software is embedded in critical infrastructures.

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?

A useful security control regime is one that is based on standards. The regime must have the participation of critical stakeholders, including the major carriers, the U.S. Government, and other governments who share a commonly held set of principles to assure the most optimal path for seamless and secure communications. It also requires a driving model, which already exists with Zero Trust. Security controls are the best practices embodied in standards. These remain useful as guides but need to be understood and implemented in the context of 5G communications. An example is asset management. NIST SP 1800-5 and ISO 27001 Annex A.8 define asset management as a core component of implementing a security policy for protection. This definition makes perfect sense in an IT enterprise with a single accountable owner. In mobile, cloud-centric 5G implementations, the assets are a combination of physical devices and virtual functions that can span many different kinds of system domains owned by many different kinds of technology and service providers. In other words, there are many owners. The requirement for asset management remains valid but implementation must adapt to the 5G architecture that is highly virtualized and is a many to many operations.

There is need for a strong level of cooperation between all resource owners on the network to make sure the data flows securely and without interruption. Trust in a 5G scenario requires a neutral central broker to deliver trust interoperability and trust governance, a means to validate authentication and authorization status in real-time, and broad adoption of zero-trust principles. If strong governance cannot be established, the efficient and scalable Zero Trust Architecture will not be realized.

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?

There are many examples of stakeholder-driven approaches that the U.S. Government is already involved in, including the U.S. NERC/FERC relationship that can be considered. Another example is the TL9000 quality management system and the handbook used by the telecommunications industry to adhere to industry standards of quality and interoperability. There are other examples including the airline industry. The right approach is a combination of private and public sector stakeholders operating within a commonly adopted governance structure.

From these examples, we can recommend a governance framework that is based on adoption of existing security standards and principles. Standards would come from existing and respected bodies including the National Institute of Standards and Technologies (NIST), the Internet Engineering Task Force (IETF), the American National Standards Institute (ANSI) X9

cryptographic standards committees, the International Organization for Standardization (ISO) and the General Data Protection Regulation from the European Union to safeguard privacy.

Principles would include cross-domain trust interoperability in 5G end to end connections, supply chain security and provenance, as examples. Again, the Prague 5G Security Conference of May 2020 is a good place to start in adopting principles to guide the development of a framework for 5G security adopted by members who have shared values in definitions of trust and want to promote the potential of a 5G driven global economy.

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?

There is a need for incentives as explained above in Line of Effort One. Closing the gaps will require the financial incentives of the U.S. Government acting as a major engine of R&D that will lead to adoption with the U.S. Government as an initial major buyer of the 5G technologies and services. This can incentivize the private sector to make the investments in the 5G infrastructure leading the way for adoption of those solutions in the private sector for advanced use cases in manufacturing, transportation and energy as examples. The U.S. Government can also be a major advocate for the governance model but will need to exercise a light hand as a critical stakeholder in ways that will be welcome by the international community to gain the widest possible adoption.

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

SecureG has no comment to offer on the economic risks associated with a 5G infrastructure

1) What opportunities does the deployment of 5G networks worldwide create 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?

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

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?

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?

Interoperability is a fundamental requirement for 5G. With the ideas proposed to the earlier questions there is an opportunity to lead in this vital area. 5G infrastructure is only in its early stages of deployment and it remains uncertain how a framework for operating interoperable trust between countries will work implementing the 3GPP R15 security protocols. There is a chance to lead. We can leverage the body of experience from other areas such as the Domain Name Service (DNS) and the Resource Public Key Infrastructure (RPKI) where the U.S. played a key role to propose a 5G (and future 6G+) PKI global CA bridge operating as the trusted third party.

Examples exist historically in the interoperation among different military coalition members cooperating in a theater of operation. In these cases, there was a lead nation to supply the communication equipment that all would use. The Zero Trust Architecture allows international cooperation and coordination. In this example, each nation uses their own equipment, but only to certain levels of trust based upon the equipment used. This 'bring-your-own-communications' is highly desirable to all nations because it allows them to make their own choices based on their own requirements. Further, the Zero Trust Architecture with provenance features allows the information to be shared with only the authorized parties, and only if it is adequately protected as defined by the originating nation's policy.

It requires a participatory form of governance as with the example of the internet domain name security. It works serving as a fundamental requirement for living in a modern society that requires global connections.

The goal is a national infrastructure that is interoperable with the global mobile communications infrastructure where security is part of the standard, but its application can be contextual. Not everything requires the highest levels of security. Context is an important element of security so users of 5G can make the appropriate trust decisions.

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

U.S. private sector participation in global standards development including 5G technologies has been plagued by being underinvested and failing to have a unified strategy to the nation's

security in the telecommunications critical infrastructure. Funding has been a key problem. U.S. companies don't take a long-game approach to supporting its representatives in standards committees and treat their experts as the most dispensable when the company runs into hard times. Where the U.S. Government can help is by taking a strategic approach to the communications sector as a key element of its economic security. This means funding companies to find its best experts and taking a long-term commitment to their participation. Contract vehicles such as Small Business Innovation Programs can be part of the answer even extending this form of contract to the larger businesses to hire and keep the standards experts.

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?

The principle of provenance is one way, as explained in previous questions. This kind of information available to the buyer of the 5G network slice (as an example) can be used in the contract agreement. The agreement would make binding that a high trust (high assurance plus high availability) connection path will require path assurance that the connection technology is on an approved list appropriate for the level of trust.

Also, not everything can be decided in advance and the technical details require governance processes in support of governance policies so that the member participants can have a say in the deliberations. Trust is not binary, and the details of the selected technology, how employed, connected and how the technology is updated matter in making trust determinations. A measure of success within North America is the degree of participation within the governance group described above. It is worth noting that participation in governance is about the operational mechanisms to ensure interoperability; this is a separate, and necessary aspect of governance that is not done by the standards organizations. Governance should follow the standards, so the same mechanisms mean the same thing across the North American or allied implementations.

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?

Governance must allow participation from stakeholders around the world. By allowing their participation, we will move much more strongly into a globally interoperable 5G network.

5) Both the Department of Commerce and the Federal Communications Commission (FCC) have rulemakings underway to address the security of the telecommunications. Are there other models that identify and manage risks that might be valuable to consider?

The multi-stakeholder model as described in previous questions is what will create the necessary trust interoperability implementing the 3GPP security requirements. The U.S. Government can consider forming a 5G Security Alliance for security interoperability across industry sectors with specialized groups within Sectors to work on specific forms of

implementation. Enforcement is also required. While the rules being developed will offer some direction, without the means to enforce those rules via solid governance that includes enforcement will only result in increased levels of bureaucracy and potential cheating.

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

SecureG has no comment in response to this question.

Contact Information:
Carlos C Solari
VP, Product Engineering
carlos@secureg.co
www.secureg.co