



June 25, 2020

Ms. Kathy Smith
Chief Counsel
National Telecommunications and Information Administration
1401 Constitution Ave. NW
Washington, DC 20230

Re: Comments on the National Strategy to Secure 5G Implementation Plan

Dear Ms. Smith,

BSA | The Software Alliance appreciates the opportunity to respond to the National Telecommunications and Information Administration's ("NTIA") Request for Comments on the National Strategy to Secure 5G Implementation Plan.

BSA is the leading advocate for the global software industry. Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing, artificial intelligence ("AI"), and other products and services that will form the backbone of 5G network infrastructure and services. In the United States, software contributes \$1.14 trillion to US GDP and supports 10.5 million jobs, with an impact in each of the 50 states and across a range of industries.¹ As major providers of the software tools, cloud-based services, and other key elements of 5G networks, BSA members are invested in capitalizing on the benefits of cloud computing and software to enhance trust and security and unlock the benefits of 5G technology.

5G networks are fundamentally different from previous generations of communications technology. Whereas previous iterations of communications networks have relied upon hardware components that quickly become outdated, 5G leverages software and cloud infrastructure to "virtualize" network functions. In fact, so important will cloud services be to 5G that many have referred to 5G as the "cloudification" of telecommunications. Virtualization and cloudification of network functions will unlock myriad new possibilities for managing and securing networks. For example, software-defined networks will enable the creation of tailored virtual environments that apply security controls customized to the data and devices used within the environment.

Because software will play such a unique and transformative role in the 5G ecosystem, 5G policy must begin with the recognition that software developers must be central in 5G stakeholder discussions. Traditional models for telecommunications policymaking are inadequate to address the fundamentally different 5G architecture and will need to evolve a greater focus on the functions and opportunities software will bring. As the Administration

¹ BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

considers how to implement its National Strategy to Secure 5G, it must begin by putting software front and center.

BSA offers the below comments as input to the National Strategy to Secure 5G Implementation Plan. We believe leveraging the inherent security benefits of 5G and the power of software can help the Administration secure 5G networks through five key lines of action: harnessing software innovation, securing the 5G ecosystem, managing supply chain risk, hardening the cloud, and building 5G governance. The Administration can lay regulatory groundwork as needed to enhance the fundamental improvements to security that are part of 5G networks.

I. Harness Software Innovation

As the backbone of 5G networks, innovative software-powered tools and techniques will fundamentally reshape how 5G networks operate – and how they can be secured. 5G networks embrace software solutions to security challenges, and the government should lead the adoption of such solutions. Specifically, investing in technologies to virtualize network functions, using new software innovations to enhance cybersecurity, and prioritizing security in 5G research and development will all maximize the impact of security efforts related to 5G networks.

Radio Access Network (RAN) technology offers one important example of the way that software can be leveraged to address security challenges. The RAN market is currently dominated by a handful of vendors, some of whom have been associated with supply chain security concerns. Virtualizing the RAN – through approaches such as Virtualized Radio Access Network (V-RAN) and Open RAN technologies, has unlocked competition and advance security at the network's edge.

Likewise, software-based technologies such as Software-Defined Networking (SDN), Network Slicing, and Network Function Virtualization bring new opportunities to mitigate cyber risks. Policymakers should develop guidance, invest in research and development (R&D), and pilot promising approaches to apply these technologies to new security techniques to segregate suspicious traffic, protect sensitive information, authenticate users, and address other key security needs.

II. Secure the 5G Ecosystem

Securing 5G networks requires more than just securing 5G network infrastructure—it also means securing the vast, dynamic ecosystem of devices that connect to it. The Administration should incentivize the secure design, deployment, configuration, and maintenance of systems operating on 5G networks to ensure true end-to-end cybersecurity.

Because 5G is powered by software, mitigating the risk of software vulnerabilities will be more important than ever. To do so, the Administration should adopt guidance and best practices to help software developers and vendors produce and maintain secure software. Last year, BSA launched the *BSA Framework for Secure Software* to provide a risk-based framework for evaluating software security, based on leading industry standards and best practices.² NIST's recently published white paper on a Secure Software Development Framework, which is closely aligned with BSA's guidance, also provides an important starting point for advancing software security.

² The *BSA Framework for Secure Software* is available at:
https://www.bsa.org/files/reports/bsa_software_security_framework_web_final.pdf.

Among the most critical security tools in the 5G environment will be encryption, which will be vital to maintaining the confidentiality and integrity of the vast volumes of data transiting the networks. The Administration should commit to enabling networks and applications to use the strongest available encryption tools, and should invest in developing new generations of encryption technologies to keep pace with evolving threats or security challenges arising from the uptake of emerging technologies like quantum computing through funding for research and development and standardization.

AI and similar technologies will play a vital role in securing 5G networks, enabling identification and isolation of threats across enormous data sets, automating monitoring, supporting incident response, and more. The Administration can help AI bolster 5G security by making data sets available to train AI systems, encouraging the development of secure, transparent AI systems, and investing in AI-focused R&D.

Arguably the most transformative uses of 5G technology will be in the massive machine-to-machine interactions that will take place on the networks across billions of IoT devices. The Administration should establish policies incentivizing device manufacturers to design and maintain secure IoT devices. These policies should build upon available internationally recognized standards and industry best practices, and should adopt risk-based, outcome-focused frameworks to achieve optimal results.

Ultimately, securing the 5G ecosystem may be best approached by applying “zero trust” principles. Zero trust architectures assume that all users and data within a network could be a threat and build flexible layers of protections to mitigate those threats, ranging from supply chain disruptions to insider attacks. Building zero trust 5G environments requires decoupling hardware and software systems wherever possible, robust user authentication protocols, ubiquitous encryption, and a strong open source-driven architecture. The Administration can advance zero trust approaches through contributing to standards development, best practice guidance, and R&D. Piloting zero trust approaches to 5G security, as NIST is currently preparing to do, is an important priority in this area.

III. Manage Supply Chain Risk

Securing 5G networks requires making strategic choices about the hardware and software on that makes up the network infrastructure. Effective supply chain risk management practices limit vulnerabilities and make it easier for defenders to protect networks by applying risk-based frameworks. Risk management entails understanding risk through the identification of likely threats, vulnerabilities and potential consequences, tailoring mitigation strategies to risks, and prioritizing actions based on the most relevant and potentially impactful risks. In a similar vein, the consistency and compatibility of regulations and technical standards across national borders enables transnational cooperation and avoids disrupting innovation. The Administration should reject categorical prohibitions against the acquisition or integration of technologies simply because they are developed abroad, and instead rely on standards-based risk management frameworks.

BSA supports the “Prague Proposals” issued at the May 2019 Prague 5G Security Conference, which guide governments to pursue security objectives in a manner that simultaneously fosters competition and innovation while ensuring that security doesn’t undermine the benefits that make 5G technology so promising. The Administration can enhance the role of supply chain in contributing to secure 5G networks by adopting a risk management approach, advancing interoperability, ensuring transparent and fair supply chain policies, promoting government-industry collaboration, and driving innovation across the supply chain.

Absent exceptional circumstances, government supply chain risk management policies and their implementation should be transparent to the public, with impacted stakeholders notified about specific actions. They should also establish meaningful mechanisms for resolving disputes, including opportunities for stakeholders to appeal or protest decisions, provide defense against any alleged offenses, and remediate past concerns. Dispute resolution mechanisms create an environment of certainty and predictability without limiting tools for mitigating risk.

Government-industry collaboration can make strong contributions to strengthening security. Policies that enable governments and industry to share information, collaborate to disrupt threats, and work cooperatively to develop common solutions to shared challenges can enhance the security of 5G networks. Governments have found success in establishing joint government-industry task forces, multi-stakeholder policy development initiatives, and other collaborative forums; these models should be replicated to address supply chain priorities.

IV. Hardening the Cloud

Cloud will drive many of the security benefits of 5G, including enabling rapid deployment of mitigations, dynamic assignment of compute resources to meet security and resource demands, and greater overall network resilience. Fully capitalizing on these benefits will require secure and trustworthy cloud environments. The administration can enable these advances by adopting risk-based cloud security policies that are aligned with internationally recognized standards and working to maintain a strong understanding of the roles and responsibilities within complex cloud environments.

Securing cloud platforms must be a priority for ensuring the security of 5G networks as a whole. To do so effectively, policies must be risk-based and account for the different types of data that cloud services will handle and the different functions they will provide depending on their location within the network. Risk-based approaches ensure optimal security outcomes while maintaining necessary flexibility and adaptability to providers to meet customer and security needs within the specific context in which they operate.

Internationally recognized standards, such as the International Organization for Standardization (ISO) 27000 series or the Service Organization Controls (SOC), provide a clear, repeatable basis for assuring and evaluating cloud security. When governments align cloud security policies with these standards, they enable cloud providers to ensure a consistent basis for securing cloud environments around the world and promote technical interoperability. Moreover, they reflect consensus guidance on the best practices that make cloud services most trustworthy. The Administration should also consider establishing reciprocity agreements with other nations that maintain similar security requirements in order to make compliance activities as efficient as possible.

As cloud services become more integral to 5G networks and the many applications and services they support, the cloud environments become more complex and dynamic. Vendors offer a range of security services that customers embed within their cloud environments, such as embedded identity management or threat monitoring services. As the number of actors within a cloud environment grow, there is a risk of confusion about the aspects of security and privacy for which each actor is responsible. For example, a cloud provider may build in certain security controls, but leave it to customers to configure others; those customers may contract with embedded service providers to address some of these controls. Roles and responsibilities may also differ across different types of cloud services, such as Infrastructure-as-a-Service or Software-as-a-Service. The Administration must ensure that

5G security policies enable careful distinction of roles and responsibilities within such complex environments.

V. Build Smart, Effective 5G Governance

Strong security controls and technical measures rely upon effective 5G governance, particularly regarding the technical standards that underpin 5G development. 5G governance will require cooperation between nations and between different government agencies within nations, particularly in the United States. To establish mechanisms for responsible governance of 5G networks and supporting technologies, the Administration should support the development and adoption of open standards with built-in security, cultivate open-source solutions, and ensure an approach to 5G governance that is flexible and coordinated across affected agencies and other stakeholders.

Open standards promote interoperability – ensuring transparency and consistency in implementations and enabling technologies from one vendor to communicate with those of others; conversely, proprietary standards support closed, proprietary systems. Interoperability is essential to ensure that network operators gain increased visibility into network traffic, and that users have diverse options for security tools. When open standards build security in – a vital priority – they drive a consistent level of protection across diverse networks. For secure, open standards to take root, the Administration must invest greater resources in supporting U.S. government agencies' engagement in standard development organizations and build processes that build collaboration on standards development with industry partners.

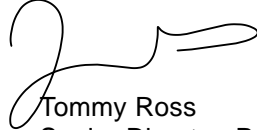
The Administration should incentivize development of trustworthy open source-driven architectural solutions by supporting the establishment of open source licensing and governance regimes and pressing for standards that support open source. Open source-driven architectures can speed innovation and reduce costs, creating a more open, dynamic marketplace. From a security standpoint, such an approach has the potential to improve transparency into critical code and potential vulnerabilities and can reduce risks of supply chain attack by decoupling hardware and software ecosystems. To realize these benefits, the Administration should invest in initiatives, including targeted R&D, to improve confidence in the security and trustworthiness of open source solutions.

As 5G becomes increasingly critical across numerous sectors, there is a risk of incoherent and overlapping governance. 5G will be a critical technology in the communications sector, the transportation sector (where 5G will enable broader adoption of autonomous vehicles), the health care sector (where 5G will support life-critical medical devices), the financial sector (where 5G will underpin online financial transactions), and others. Whereas previous generations of communications networks could be regulated strictly as telecommunications services, 5G depends on core infrastructure – such as cloud services – that simultaneously serves multiple functions and clients, making it a poor fit for telecommunications-specific regulations. Successful governance will require a unified approach across sectors and agencies. Such governance mechanisms must be flexible and build risk-based approaches that tailor compliance requirements to each 5G network's specific uses and threats. Multiple agencies across the U.S. government have already begun to adopt 5G policies; the Administration should act now to establish effective mechanisms to enforce coordination and coherence across agencies.

As the Administration begins to implement the National Strategy to Secure 5G, it is important to recognize the soundness of the foundation from which it begins: 5G brings innate security advantages that offer the potential to transform security and privacy for government,

business, and individual users. Harnessing these advantages will require contributions and collaboration from both government and industry, and our members are ready to meet this challenge. We look forward to working with NTIA to implement the National Strategy to Secure 5G and to promote best practices in securing 5G. Thank you for the opportunity to comment on this important matter.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tommy Ross', with a stylized flourish extending to the right.

Tommy Ross
Senior Director, Policy