Jeff Edlund
Chief Technology Officer
HPE CMS

Mr. Travis Hall
Telecommunications Policy Specialist
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, D.C. 20230

June 25, 2020

Re: Hewlett Packard Enterprise response to NTIA request for public comment on Implementation Plan for National Strategy to Secure 5G; RIN #0660-XC047, Docket No. 200521-0144

Dear Mr. Hall,

Hewlett Packard Enterprise (HPE) welcomes the opportunity to submit these comments to assist the Executive Branch in developing The National Strategy to Secure 5G Implementation Plan in accordance with the Secure 5G and Beyond Act of 2020.

HPE is an independent, publicly traded U.S. technology company headquartered in San Jose, California. We maintain a comprehensive technology portfolio that includes cloud computing solutions, data center infrastructure, IT for data and analytics, high performance computing, and networking equipment. These products provide solutions for clients in a range of industries as well as government entities, from helping small businesses move to the cloud to accelerating new discoveries in mathematical sciences to facilitating cutting-edge research into neurodegenerative diseases.

In the 5G core, we provide the building blocks for networks based on the global-leading secure industry standard servers for the telecommunications core and edge. Our specialized software is open and secure which allows telecommunications providers to evolve their networks into 5G service-based architecture. HPE is working to support the development and implementation for secure and open 5G, and offers these comments to support the Executive Branch.

Line of Effort 1: 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)?*

HPE is an advocate for government participation and promotion of policies that will create an atmosphere of open innovation in the U.S. Manufacturers and software developers must have some confidence that their investments will return meaningful business results, their intellectual property will be protected and that the U.S. participation will de-risk certain investments so the innovative power of our workforce can be unleashed. HPE sees 5 primary areas of governmental action that can

produce meaningful results:

- **Telecommunications workforce training / re-training** – The 5G network requires a mix of legacy and new skills to design, implement and support a nationwide infrastructure. The government should prioritize funding for training / re-training programs specifically designed to provide not only baseline skills for 5G at the radio, transport, edge and core layers of the network, but also provide training for development of both revenue generating and citizens support applications and services that will leverage the unique features of 5G. This approach will not only prepare the U.S. workforce for implementation of the national 5G infrastructure, but a focus toward application and service innovation can lead to U.S. dominance in the critical space of 5G value chain creation.
- **Spectrum policy both U.S. and abroad** – HPE supports government increase of both commercial and private access to shared, licensed and unlicensed spectrum for 5G and the services needed to support 5G deployments. In particular focus should be placed on realistic plans to execute against a goal of connecting everyone via the 5G network and economy. New innovations such as ATSC 3.0 can be leveraged to provide meaningful downlink for any individual that has the ability to receive broadcast TV signals. These types of innovations should be aggressively supported by policy makers and represent not only a U.S. opportunity, but present the ability to have discussions globally on potential spaces of harmonized spectrum
- **Specific investment in 5G security innovation** – 5G standalone networks are currently being sold in 2 scenarios: 1) Vertically Integrated single vendor solutions, 2) Open, Multi-vendor solutions that have been tested for function and supportability. Each approach has security problems, but a multi-vendor solution is a more secure option and U.S. government policies should promote a multi-vendor approach. While both single and multi-vendor solutions are potentially vulnerable to external exploits, because multi-vendors solutions require open and observable interfaces between the services, it is much easier to detect and mitigate any potential exploit. Observability is the key to securing the network and there are many 5G security innovations that can be developed into a value chain that can be deployed in the U.S. and sold worldwide.
- **Public funding to promote open collaboration** – Public funding should be made available to promote the open development, testing, integration and support of mixed vendor solutions. This approach would take the burden off of the telecommunications service providers to pre-test configurations prior to implementation into their networks. This approach would not only reduce costs for implementation of network features, it would also ensure that all participants are on an equal footing when testing and validating their solutions.
    - HPE has made a major commitment to 5G openness and collaboration in the U.S. HPE currently operates an Open5G lab in Ft. Collins Colorado where CSP customers, HPE partners, and 5G ecosystem players can come together for interworking, performance testing and validation of Multi-Vendor 5G solutions. The Open5G lab also provides capacity for Proof of Concept and Demonstration of 5G use cases. We are currently in discussions with ATIS to further extend a standards partnership in the lab, where ATIS would come alongside HPE and ensure that the tests run in the lab are standardized

and consistent for all vendors.
    - Currently this lab is focused on the (SBA) Service Based Architecture for 5G standalone networks. But opportunities remain to bring O-RAN compliant vendors into the lab to create and validate end to end 5G solutions.
    - HPE would welcome government participation and incentives to further accelerate the capabilities, capacity and programs available in this lab.
- **Immediate focus on 4G / 5G interworking** – Policy makers should work with industry to accelerate the pace of 4G / 5G interworking. Standards are still in development and some have yet to emerge that will cause services such as SMS (Short Message Service, a.k.a. texting) to work between 4G and 5G endpoints. Government should pursue standards organizations such as ATIS to not only facilitate the ongoing development of such standards but to pursue alignment internationally so that service experience is consistent worldwide.

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

It is vitally important that the U.S. government provide programs, financing and tax incentives superior to the actions taken in other geographies across the globe. The Chinese government and the European Union among others have been aggressively funding the development and deployment of 5G technologies and networks. In 2016 the EU presented the 5G action plan with an investment of $300 million Euros. The U.S. government should support the formation and implementation of an U.S. based approach on 5G infrastructure and supply chain similar to those considerations in the EU toolbox proposal:

- Telecommunications and cybersecurity rules
- Coordination on standardization as well as U.S. national certification
- Direct investment in a screening framework to protect the U.S. supply chain
- Trade defense measures
- Competition rules

While HPE feels that the EU toolbox approach is instructive it is necessary for the U.S. to develop its own approach which facilitates investment in technology that positions the U.S. for leadership in telecommunications now and in the future.

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 Government can promote private sector investment in 5G by providing project funding to design, test and implement not only 5G networks but 5G services. Technical and financial risk is shared between government and industry in this type of arrangement.

Adoption of investment strategies can also accelerate the time to market for tested and certified solutions. This acts as additional incentive for industry.

Hewlett Packard Enterprise

Jeff Edlund
Chief Technology Officer
HPE CMS

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.*

To obtain visible leadership in 5G the U.S. Government should look across the entire 5G ecosystem from RAN through Transport and Edge and into the core network. Increased funding should not be focused only on the RAN and O-RAN part of the 5G solution as the rest of the ecosystem is vital for bringing the entire solution to life. Research into cloudification and the limits on using cloud native technologies in the RAN and Transport sections of the network should be explored for new innovations. Government should partner with and fund industry to develop U.S. based, open, multi-vendor testing, validation and certification policies and centers where these efforts can be executed.

The US Government should also look beyond 5G and start investing and encouraging innovation in the 6G network which should start taking shape from a vision perspective in the next 7 – 10 years.

Line of Effort 2: 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?*

At the 5G Core Software layer, HPE advocates for open, standards-based methodologies consistent with today's cloud-native principles. HPE develops 5G core network functions using the open principles of the 12-factor application development methodology [http://www.12factor.net]. Among these principles are the design concepts of dataless and stateless execution allowing for development of lightweight Microservices-based components without embedded data or state information. In this model, all 5G core network functions become standardized entities incapable of performing proprietary execution without easily undergoing detection.

Additionally HPE advocates for the use of common, independent and standard security management functions for all network functions in a 5G infrastructure. Having each network function, as is often the case today, embed its own proprietary security functions results in a lack of transparency, control and audit and increases the risk of security misconfiguration and security defects in the 5G core network. The U.S. Government should encourage the standardization of the security management interfaces to network functions and their adoption. Examples of security management interfaces include key and credential management, certificate management, security policy and configuration management, and security audit log collection.

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?*

Hewlett Packard Enterprise

Jeff Edlund
Chief Technology Officer
HPE CMS

Component and sub-component supply chains that are not in the U.S. may pose a known but unaddressed source of compromised 5G infrastructure. Risks need to be addressed in priority order based on threat of compromise. Industry and government should work together to identify and analyze the risks in components and sub-components, including printed circuit board manufacturing, complex cable assemblies such as iSCSI, Ethernet, InfiniBand and others, logic bearing sub-components with internal bus connectivity to the platform such as CAN/MIC bus or other unprotected busses, or internet connectivity. Examples include fans, power supplies, disk drives and more. Mitigation and management practices and methods should be established to reduce the risks inherent in supply chain. If the U.S. Government should decide to build a network of trusted allied countries to host the component and sub-component supply chain, then government should incentivize the move of critical advanced manufacturing to the U.S. and trusted allied countries as another method of reducing risk.

The ICT supply chain and manufacturing will remain global for years to come, but in the meantime U.S secure finishing can provide safety checks of every component and sub-component. These checks include automated x-ray analysis of printed circuit boards with historical tracking against repairs, crypto graphic configuration manifests to detect transit tampering, all with background-checked U.S. citizen workers to prevent manufacturing insider threats.

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?*

Security requirements need to be complemented with security assurance tests to ensure they are in place and correctly implemented. Many security defects are caused by incorrect implementations or misunderstood requirements. We see a need for increased security tests and continuous security tests of 5G network and for suppliers to provide more ‘evidence’ of the security assurance tests they perform.

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?*

HPE integrates security throughout the product cycle, implements security policies and practices across our complex supply chain, and supports security playing a greater role in the acquisition process. Security should be as important a factor as cost, schedule and performance, and companies who invest in securing their supply chains should be recognized for those investments. We encourage the U.S. Government to set security requirements during the procurement requirements formulation process and allocating resources to ensure security is priority throughout the procurement cycle. We also believe the U.S. Government should adopt a mission-specific, risk-based approach for determining requirements for procurements. Different procurements will require differing levels of security and most civilian agencies’ security needs should be met through the declaration of conformance to international standards and internal supply chain policies and practices.

Security procurement requirements should include moving platform and components to a zero trust model. As Trusted Computer Group, NIST and others develop industry standard guidelines for zero

trust architecture, these guidelines should be added as procurement requirements for 5G infrastructure. NIST has developed security recommendations in the following Special Publications:

- SP 800-147b BIOS Protection for Server - principles for secure BIOS updates to prevent BIOS rootkit attacks.
- SP 800-193 Platform Firmware Resiliency Guidelines - extends 800-147 to provide a hardware root of trust for the platforms firmware(s), BIOS, and Operating System to prevent and detect firmware(s)/BIOS/Master Boot Record/Operating System rootkit attacks.
- SP 800-194 Platform Recovery Guidelines - Still in draft, extends 800-193 to automatically recover the platform if a destructive breech tries to perform a broad denial of service attack against the 5G infrastructure like a ransomware attack or what North Korea did to Sony Motion Pictures that took several weeks to recovery from.
- SP 800-207 Zero Trust Architecture – still in draft, principles of zero trust for enterprise infrastructure, workflows, networking and is applicable to 5G infrastructure and 5G core networks.

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 U.S. Government and industry should work together to assess risks to the ICT supply chain. The government should incentivize moving areas of high risk to the U.S. and to allied countries, when they are identified by government and industry.

Line of Effort 3: 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?*

Consistency of application execution across 5G cores worldwide due to standardization of core components enables enterprises to service a broader, borderless marketspace. Network Slicing, combined with edge-core deployments provides localization of near-real-time services as has been seen already from the formation of the Microsoft Azure edge-cloud world-wide service provider arrangements and Amazon Cloudfront edge locations.

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

Mitigate and eliminate risks associated with embedded, proprietary implementations of 5G Core capabilities by embracing an open Microservices architecture for the 5G Core that utilizes independent and separate data and state information associated with all call processing actions within the core.

Hewlett Packard Enterprise

Jeff Edlund
Chief Technology Officer
HPE CMS

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

- Guide Communication Service Providers [CSPs] and enterprises alike to embrace open architectures which promote common application development, deployment and distribution.
- Focus on the use-cases possible with the 5G core when that core becomes a common entity across all CSPs and Enterprises.
- Create a level playing field for all 5G core vendors by promoting a mixed and multi-vendor environment within CSPs and Enterprises in order to eliminate the risks associated with a single-source supplier.

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?*

HPE supports government increase of both commercial and private access to shared, licensed and unlicensed spectrum for 5G. In particular focus should be placed on realistic plans to execute against a goal of connecting everyone via the 5G network and economy. New innovations such as ATSC 3.0 can be leveraged to provide meaningful downlink for any individual that has the ability to receive broadcast TV signals. These types of innovations should be aggressively supported by policy makers and represent not only a U.S. opportunity, but present the ability to have discussions globally on potential spaces of harmonized spectrum

HPE recommends that the USF craft future unlicensed spectrum allocations in such a way that favorability is provided to those entities demonstrating open, mixed / multi-vendor environments.

Further we encourage more private 5G and 4G deployments using unlicensed spectrum where the use-cases are clearly defined around open core environments so that any potential proprietary actions are immediately revealed / eliminated.

Line of Effort 4: 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?*

- Encourage U.S. companies to actively participate in the overall standards development activities associated with 5G structural and procedural definition.
- Begin a U.S. program focused on the 3GPP Release 17/18 definitions with a targeted approach toward 6G and beyond initiatives.

Hewlett Packard Enterprise

Jeff Edlund
Chief Technology Officer
HPE CMS

- Encourage private company exploration of edge deployments utilizing unlicensed 4G and 5G spectrum by implementing an incentive program around the incorporation of mixed/multiple U.S. company components in the end-to-end solution.
- Target key industries (V2x, centimeter-mapping, AR/VR) as leading entities in development of use-cases through government incentive programs.
- Encourage agricultural development activities through farm-based subsidy programs where the use of private spectrum and 5G use-cases are established and deployed.

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

- The Government should provide a grant-based incentive package for those enterprises capable of simultaneously defining new 5G use cases coupled with open standards methodologies.
- Establish an incentive package for those opportunities resulting in standards definition and adherence across broadly accepted standards-bodies (3GPP, IETF, IEEE).
- Provide U.S. Government-directed guidance into operator-defined governing bodies such as the Next Generation Mobile Network Alliance, 5G Americas, and the Wireless Broadband Alliance, and couple such guidance with feedback from impacted / interested / involved U.S. Supplier vendors

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 U.S. Government should ensure / mandate an open environment across all 5G core components to establish a baseline means of reporting and accountability across all supplier vendors and associated communication services providers operating the 5G Infrastructure. Private enterprises utilizing an associated private 5G core must undergo auditing and validation to ensure openness and interoperability. Create a validation working environment to ensure standardized methods of delivery, update and execution of any and all Core Network operations.

The above approach in combination with HPE recommendations in section 1 in regards to the support and participation in a national 5G test lab will create the most open environment and ecosystem that can be secured through observability at every segment of the 5G solution.

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?*

Creation of a U.S. government grant structure commensurate with the usage of private spectrum resources whereby enterprises are required to demonstrate open and common 5G core definition, deployment and execution. Establish a reward-system for new 5G use cases capable of clear

demonstration of 5G core openness and interoperability.

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?*

Given the importance of 5G to the U.S. economy, Government and industry should share the goals of mitigating cybersecurity threats to mobile network infrastructures, prevent cyberattacks and reducing the impact of related cybercrime. Achieving these goals will be a collective effort. Technical measures that mitigate security risks to mobile network infrastructures, applications, services, and the operators' customers and end users – including both consumers and enterprises – exist and should be incorporated into government planning.

In January 2020, the European Commission endorsed the joint "5G Toolbox" of mitigating measures for use by EU Member States to address security risks related to the rollout of 5G.

Recently, GSMA collaborated with a group of service providers and vendors to develop a new security reference document, FS.37, which highlights best practices for securing 5G networks. This document outlines recommendations for service providers for detecting and preventing attacks on the GPRS Tunneling Protocol User (GTP-U) plane against mobile networks, services and applications. It provides recommendations for service providers on how to address the threat posed by malware and vulnerabilities, including specific examples, contains guidelines on how to logically deploy security capabilities, including specific interfaces, and the modes of deployment. It also briefly introduces new topics, such as the concept of security per network slice.

---

[4] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, Proposed Rule, 84 Fed. Reg. 65316 (Nov. 27, 2019) (implementing Exec. Order No. 13,873, *Securing the Information and Communications Technology and*

Recently, GSMA collaborated with a group of service providers and vendors to develop a new security reference document, FS.37, which highlights best practices for securing 5G networks. This document outlines recommendations for service providers for detecting and preventing attacks on the GPRS Tunneling Protocol User (GTP-U) plane against mobile networks, services and applications. It provides recommendations for service providers on how to address the threat posed by malware and vulnerabilities, including specific examples, contains guidelines on how to logically deploy security capabilities, including specific interfaces, and the modes of deployment. It also briefly introduces new topics, such as the concept of security per network slice.

A strong security posture is critical for a successful digital transformation. Service providers need to have constant real-time visibility and granular control across traffic passing through their networks in real time. It is HPEs opinion that this is only achievable in open, observable multivendor 5G solutions versus closed or proprietary and vertically integrated single vendor solutions.

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

HPE would recommend the appointment of a new office in government specifically tasked with leading and coordinating efforts across all agencies for the development, deployment, support and security of 5G in the U.S. The new office should equally be concerned with coordination of efforts with other national governments across the globe.

Any and all efforts should be taken to remove competition and duplication between government agencies working on different but related initiatives in 5G or future Telecommunications opportunities.

HPE would recommend attention be given toward future connectivity needs and that government and industry partnership start working strategy and innovation on 6G now ahead of the emergence and framing of standards.

5G promises to revolutionize the technological, industrial and societal landscape. HPE is uniquely positioned to help the U.S. lead in the development and deployment of a secure and open 5G infrastructure. We appreciate the opportunity to participate in developing and executing a strategy to make this goal a reality.

Jeff Edlund
Chief Technology Officer
Communications and Media Solutions
Hewlett Packard Enterprise