Cisco Systems, Inc.
601 Pennsylvania Ave. NW
Washington DC 20004

Phone: 202.354.2904
www.cisco.com

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC. 20230

In the Matter of The National Strategy to Secure 5G Implementation Plan	)))))	Docket No. 200521–0144

COMMENTS OF CISCO SYSTEMS, INC.

Eric Wenger, Senior Director
Mary Brown, Senior Director

CISCO SYSTEMS, INC.
601 Pennsylvania Avenue, NW
9th Floor, North Building
Washington, DC 20004
202.354.2904

June 25, 2020

TABLE OF CONTENTS

Cisco Systems, Inc.
601 Pennsylvania Ave. NW
Washington DC 20004

Phone: 202.354.2904
www.cisco.com

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC. 20230

In the Matter of	)	
	)	
The National Strategy to Secure 5G Implementation Plan	)	Docket No. 200521–0144
	)	
	)	

COMMENTS OF CISCO SYSTEMS, INC.

Cisco Systems, Inc. ("Cisco") hereby submits its comments in response to the Notice and Request for Comments ("Notice")[1] by which the National Telecommunications and Information Administration ("NTIA") seeks input to inform the development of an Implementation Plan for the National Strategy to Secure 5G in accordance with the requirements of the Secure 5G and Beyond Act of 2020.[2]

INTRODUCTION AND SUMMARY

Cisco thanks NTIA for its leadership in developing both strategies and implementation plans critical to the successful build-out, deployment, and use of 5G networks. Cisco believes that advanced wireless networks, including 5G, have the potential to enable a new wave of innovation and competitive opportunities for American industry. Like every generation of wireless mobile data communication technology before it, 5G offers a potential new set of capabilities that can power new use cases. With regard to 5G—and the complementary technology in Wi-Fi6—these

[1] National Telecommunications and Information Administration, *The National Strategy to Secure 5G Implementation Plan*, Notice, Request for Public Comments, Docket No. 200521–0144, 85 FR 32016 (May 28, 2020). https://www.govinfo.gov/content/pkg/FR-2020-05-28/pdf/2020-11398.pdf

[2] Secure 5G and Beyond Act of 2020, Pub. L. No. 116-129, 134 Stat. 223 (2020), https://www.congress.gov/116/plaws/publ129/PLAW-116publ129.pdf.

include higher bandwidth, lower latency, and greater device density. The U.S. government can play a critical role in helping industry understand the import of these new capabilities—as well as the challenges and opportunity their use will bring. Therefore, as described below, Cisco urges the federal government to: (1) promote agility, dynamism, and innovation by raising awareness about potential new 5G use cases; (2) leverage testbeds for rigorous assessments of security performance in various operational scenarios; and (3) implement the National Strategy internationally to ensure the development of a diverse global ecosystem of 5G equipment and services.

5G is not just about high-speed data connections for enhanced consumer mobile broadband. 5G will deliver that, of course. It will also enable entirely new service models—and new revenue opportunities—for operators who successfully leverage the new capabilities of 5G to identify, build, and deliver the most compelling use cases. Those use cases in turn may serve as a platform for a new generation of entrepreneurs to develop innovative business models beyond our ability to forecast from where we sit today. However, without greater understanding of the most compelling use cases, decisions we make in the near term about network architecture may constrain future feasibility of some use cases.

Advancements delivered via 5G technologies allow for new flexibility in the configuration and use of advanced wireless networks. These include separation of the control plane from the data plane, movement of more intelligence to the edge of the network (multi-edge access compute), and the ability to deliver customized "network slices." New configuration options bring both new challenges in terms of how to properly protect connected devices and also new opportunities to improve security by leveraging the power of intelligent, intuitive networks. If properly architected and configured, the capabilities of next generation networks can deliver better security than is possible today. Greater levels of visibility and control over the movement of data and the operation

of devices can allow for cloud-based implementation of "Zero Trust" security, including role-based access controls, device isolation, and network segmentation.[3]

Advancements offered 5G network cores will be necessary to take full advantage of the massive throughput and low latency that new 5G radios provide at the edge. Core networking innovations will allow public mobile network operators to leverage major changes taking place in data centers, networking, and the economics of mobility in a standardized multivendor environment. These significant changes will facilitate new opportunities such as personalized networks through slicing and more granular functions. Greater levels of reliability and resiliency can also be achieved.[4]

Cisco is developing its mass scale 5G solutions with operator needs in mind. Cisco's strategy is to transition its customers to a cloud-centric network. Cisco believes 5G is not just about new radios and faster consumer mobile broadband. It is about the total end-to-end network that will provide service in a wide variety of use cases for enterprise and industrial customers with orchestration from the cloud.

The ability of mobile network operators to select from a wide range of options for their 5G service offerings also means there will be a broad array of choices for how best to architect their 5G networks. Decisions about which capabilities should be emphasized, and, therefore, which architectures should be prioritized, will to some degree rely on discerning which 5G dependent services will drive market adoption. This in turn explains the importance of federal government

[3] "Operators can now apply innovative methods to correlate geo-location information to behavioral analytics, compare those against policy in the context of a threat to the carrier cloud, and ascertain the nature of that threat and what to do about it with far greater clarity. Visibility and control properly applied to the advanced threats of today offer the carrier cloud a level of protection." https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf

[4] "Cisco and Telstra have completed a world first with a 5G Sub 6 GHz radio call over a packetized fronthaul network (X-HAUL) utilizing Cisco segment routing to improve network resiliency for Telstra customers." https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2058724

efforts to develop greater understanding of 5G use cases beyond faster delivery of movies and games to consumer mobile handsets.

In this sense, the "Race to 5G" does not well describe the transition in networking that 5G presents. It is not simply a "race" to install 5G radios at base stations that provide nationwide coverage, or to reach a certain number of 5G small cells. In fact, the characterization of 5G as a race can lead to prioritization of cost and speed over other critical priorities, such as security and functionality.

Rather, it is more of an exploration of uncharted territory as new technology begins to be applied to new problems. The transition to 5G will happen in waves or phases over many years. As we will discuss in greater detail below, the first critical part of that effort requires allocation of spectrum. 5G networks will likely be made up of various blocks of spectrum, each with different characteristics. As we discuss further below regarding the need for advancements in smart sharing of spectrum, Wi-Fi and other unlicensed spectrum technologies are critical to the success of 5G and next-generation wireless networks.

Today, connectivity through Wi-Fi and 4G LTE is complementary, and 5G industrial and enterprise environments will take this further, offering the possibility of selecting between or combining connectivity through a variety of licensed and unlicensed spectrum through multiple different radios managed by both mobile network operators and enterprise private networks. The Federal Communications Commission's planned release of additional mid-band spectrum for unlicensed use in the 6 GHz band will improve the capabilities of advanced Wi-Fi offerings, including the latest generation of Wi-Fi technology, Wi-Fi6.[5]

[5] *Unlicensed Use of the 6 GHz Band*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3852 (2020).

Once spectrum is allocated by national governments, two key areas of network development will be possible—the deployment of new radios at the edge of the network and the refresh of the mobile network core. Once 5G radios can be deployed and handsets or other devices can be sold, network operators will be able to deliver impressive boosts in transmission speed, markedly reduced latency, and much greater device density by virtue of the increased reliability of the Radio Access Network ("RAN").

However, the most revolutionary changes associated with 5G technologies will require reimagining the core of today's mobile networks. This transition will move the market from what is termed "non-standalone" 5G networks to networks that are "end-to-end 5G" or "standalone 5G." In fact, Cisco has had 5G core technology available in the market for several years, and we look forward to accelerating the transition to end-to-end 5G.

Cisco supports the NTIA's efforts in this proceeding and elsewhere to ensure the development of secure and reliable connectivity through its National Strategy to Secure 5G.

I. IMPLEMENTATION OF THE NATIONAL STRATEGY TO SECURE 5G REQUIRES USE CASES THAT ADVANCE AGILITY, DYNAMISM, AND INNOVATION

A. The Administration Should Advance a Light Touch Regulatory Framework that Streamlines Deployment and Encourages Open and Interoperable Technology

The Administration can best facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem by establishing and maintaining a light touch regulatory approach that expedites deployment[6] and fosters powerful global market-

[6] Cisco supported the Commission's most recent resolution of network neutrality rules. *Restoring Internet Freedom*, Declaratory Ruling, Report and Order, and Order, GN Docket No. 17-108, 33 FCC Rcd 311 (2018). But there is more work to do. While the FCC has made improvements in enabling service providers to plan and deploy 5G networks by creating guard rails for municipal antenna siting permits, municipal regulations are in many cases not online; digitization of these requirements would greatly facilitate planning.

based trends towards open and interoperable consensus-based standards in 5G hardware and software. Along with the spectrum advances we discuss below in Section I.B, regulatory certainty around these principles would dramatically accelerate domestic deployment and stimulate innovation favoring network operators and suppliers based in the United States and allied countries.

For instance, one particularly promising area of innovation derives from opening up the RAN. Open and interoperable RAN ensures that network operators that are investing in new infrastructure and network upgrades through the transition to 5G have a competitive and diverse set of choices among innovative and trusted suppliers providing secure 5G. Open and interoperable RAN ensures that radio selection does not lock a service provider into other network elements from the same vendor.

Adopting an open system attempts to avoid defining key interfaces in ways that may inhibit competition among suppliers. In an open system, when new innovation in the radio occurs, existing radios can be swapped out—or simply upgraded in place via software—without necessarily requiring downstream parts of the network to be changed as well. This facilitates competition, innovation, and "best of breed" choice among available technologies, while reducing barriers to entry for new players. Entrepreneurs do not need to rely upon adoption of their innovations by a limited number of radio manufacturers and can sell directly to service providers. Furthermore, a substantial portion of the advancements in this field will be in software and cloud-based services—areas where American companies historically excel.

Cisco disputes assertions that open RAN technology will not reach a sufficient level of maturity to permit widespread adoption in the market until it is capable of being fully integrated with the hardware at the edge of the network. Such claims significantly undersell the maturity of

existing technology.[7] Open RAN systems are already deployed in major markets in Japan, Europe, and India and are the subject of testing and trials by operators in the field, with new companies building upon the open interfaces of open RAN to develop new and innovative radio hardware and/or software solutions that will dramatically enhance network performance and economics.[8] The time is ripe now for the encouragement and development of open systems.

To be clear, we are not calling for government mandates; we do not want the U.S. government—or any government—to force a shift to open RAN or any other approach to building a network.[9] Instead, we urge the U.S. government to promote a regulatory model that provides for streamlined deployment and encourages diversity and choice among rigorous standards-based innovations in the market of trusted suppliers.

---

[7] "Cisco, Altiostar and World Wide Technology (WWT) are working together on an open, virtual radio access network (vRAN) blueprint for service provider networks. The joint solution will help carriers deploy cloud-based vRAN systems based on technologies from Cisco and Altiostar and that will be brought to market using the sales and integration capabilities of WWT." https://www.fiercewireless.com/wireless/cisco-altiostar-and-wwt-team-open-vran

[8] Comments of The Open RAN Policy Coalition, WC Docket No. 18-89 at 7-8 (filed May 20, 2020). Examples of open RAN deployments include: (1) Rakuten has deployed a commercial fully cloud-native mobile network with open vRAN in Japan, with radios and other equipment, software, and services from multiple vendors. Initially built with 4G radios, 5G capabilities will be deployed via software upgrades of existing Altiostar radios and 5G radio hardware from NEC. The network will be powered by Cisco's telco cloud, core, routing, switching, and services; (2) Altiostar has deployed its software with 4G/5G radios from Airspan, MTI, Nokia and Sercomm and is working with radios and related equipment and materials from Flex, Fujitsu, KMW, NEC and Xilinx to deploy by mid-year; (3) Indian integrated telecommunications services provider, Bharti Airtel, has deployed Altiostar's open vRAN solution across multiple major cities in India; (4) DISH Network is building the United States' first software-defined 5G wireless broadband network utilizing an open, intelligent RAN architecture, and DISH has entered into a multi-year agreement with Mavenir to deliver cloud-native open RAN software; (5) Mavenir has deployed with Vodafone Idea; (6) NTT DOCOMO has already realized interoperability between base station equipment of Fujitsu, NEC and Nokia with O-RAN Alliance-compliant fronthaul and X2 interfaces in their 5G commercial service; (7) Telefónica has established an open RAN consortium of hardware and software companies aimed for the development and deployment of open RAN in 4G and 5G, comprising the necessary design, development, integration, operation and testing activities required to materialize open RAN; and (8) Parallel Wireless, Mavenir, and Altiostar have been deploying Open RAN with operators such as Vodafone, Telefonica, MTN, Optus. In addition to these real-world deployments, there are numerous trials, demonstration projects, and standards development activities presently underway worldwide to advance open RAN. *See also* https://www.openranpolicy.org and https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/elastic-services-controller-esc/reimagining-mobile-network-white-paper.pdf

[9] Comments of The Open RAN Policy Coalition, WC Docket No. 18-89 at 4 (filed May 20, 2020) (arguing that "while the Commission should indeed leverage this proceeding to give new solutions an opportunity for deployment, the Commission should not pick winners nor mandate replacement decisions.").

B. The Administration Should Develop an Agenda for Research and Data-Based Improvements to Maximize the Efficient Use of Spectrum

The Administration also must encourage spectrum sharing and develop innovative means of effective utilization of available spectrum for 5G. Cisco believes this is an area that holds enormous potential to accelerate and leverage the benefits of U.S. deployment, and we outline our specific recommendations below.

First, the federal government should urgently conduct more research regarding the propagation models for various types of spectrum and common problems in propagation, such as the effect of building entry loss or ground clutter. This research should cover the various radio deployments and environments of today's mobile networks, e.g., high mobility user equipment and devices (UEs) and low mobility UEs, high UE concentration environments and low UE concentrations, along with the impacts of advanced beamforming and similar advanced radio propagation features. Such knowledge is foundational to crucial policy decisions about what bands of spectrum should be the focus of deployment; what barriers in terms of incumbent users must be addressed to enable wide scale deployment and use; and whether and how smart sharing of currently allocated spectrum can be enabled.

While there are ITU-R models on these topics, many of them are the result of unsystematic data inputs and committee negotiation. As such, they represent "rough estimates" or "best guesses" of how radio energy propagates and, in some cases, do not reflect today's advanced 5G radio features. Our inability to rely on improved, data-driven analysis is severely handicapping our use of available spectrum. For all users of 5G, whether they are commercial or government, we urgently need to derive an improved understanding of propagation and interference, both for co-channel spectrum sharing (when clearing is not possible) and adjacent channel interference (enabling better choices about when services can operate adjacent to one another without causing

interference). While it may appear at first glance that the government has few incentives to enable smarter sharing in or around bands it uses or plans to use, we believe that, in fact, the opposite may be true. Greater knowledge about wave propagation could potentially reveal new mechanisms for more effective sharing available of spectrum without undue risk of disruption to incumbents.

As of now, our ability to share spectrum, while more advanced than ever before, remains primitive as compared to the possibilities that we believe exist. We can share geographically by putting one transmitter in one location, and then separating a second transmitter geographically to avoid harmful interference, and also by using automated databases that can change channels quickly in response to protected transmitters shifting their positions, as in CBRS. There are also successful examples of sharing via ultra-wideband radio underlays. However, this is not enough to accommodate the innovation that is possible in this field.

We need to develop more tools in this arena through the application of artificial intelligence or other data-driven approaches such as sharing the same spectrum but separating transmissions in time. As of today, radios are designed by humans and when they are deployed in the world, the waveforms utilized do not change. If waveforms could change in response to dynamic interference environments through the use of artificial intelligence, it may be possible to wring more efficiency out of the available radio spectrum.[10] More accurate propagation data, such as improved clutter loss modeling or hard data about building entry loss for the various radio deployments and environments of today's mobile networks, is indispensable to these improvements.

In short, the Administration should think expansively about spectrum sharing and work with industry stakeholders to explore new use cases that experiment with new propagation models

[10] *See* "The Radio Frequency Spectrum + Machine Learning = A New Wave in Radio Technology," Defense Advanced Research Projects Agency (DARPA) (Aug. 11, 2017), *available* at https://www.darpa.mil/news-events/2017-08-11a; "How AI is Starting to Influence Wireless Communications," IEEE Spectrum, *available at* https://spectrum.ieee.org/computing/software/how-ai-is-starting-to-influence-wireless-communications.

and improved data.[11] Additionally, the Administration should work with industry stakeholders to push toward more efficient use of the radio medium more broadly, including user equipment and new radios. For instance, encouraging beam forming and other engineering improvements would increase the efficient use of spectrum. These possibilities should be at the heart of the Implementation Plan for the National Strategy to Secure 5G.

C. The Administration Should Leverage Testbeds and Government Deployment to Explore New Use Cases

The transition from 3G to 4G was largely about increased speed to consumer handsets, which enabled video-intensive services like Netflix. Likewise, the transition from 4G to 5G will further boost speed, reduce latency, and increase device density, which will improve consumer end-user experiences. However, Cisco forecasts that the most dramatic changes resulting from 5G technologies will come from its uptake by industrial and enterprise customers, who will benefit from innovations in multi-access edge computing (moving intelligence to the edge of the network) and network slicing (guaranteeing delivery of connectivity with specific, customizable properties).

Today, Wi-Fi and 4G LTE exist as complementary technologies. Mobile devices grab available Wi-Fi connectivity when cellular signals are weak (e.g., indoors). Mobile networks offload IP traffic to Wi-Fi and fixed networks to optimize performance. In the 5G future, though, industrial and enterprise users of spectrum will select between or even combine elements of three delivery models for connectivity to devices on their networks, likely through access points inside of buildings that combine multiple radios that accommodate both 5G and Wi-Fi technology and utilize: (1) licensed spectrum managed by a service provider; (2) licensed spectrum dedicated to

[11] For instance, high mmW and terahertz frequencies are ripe for propagation research and exploration of use cases. The FCC has opened this spectrum for use by innovators, but far more attention needs to be paid to the development of use cases, and in understanding radio wave propagation of this spectrum. *See Spectrum Horizons*, ET Docket No. 18-21, First Report and Order, 34 FCC Rcd 1605 (2019).

private use, which is then managed by the industrial or enterprise customer or by the service provider on behalf of that customer; and (3) unlicensed spectrum managed by the service provider, industrial or enterprise customer. Potentially, networks using both 5G and Wi-Fi technology could be provided by either traditional wireless network operators or networking companies, like Cisco, working with RAN partners or other 5G integrators or vendors to provide the service to the industrial or enterprise customer as a private 5G network.[12]

To advance these innovative possibilities in enterprise autonomy, the Implementation Plan should actively explore different industrial and enterprise use cases for 5G that go beyond simply delivering faster wireless broadband to the consumer. These use cases may include:

- ***Ultra-reliable low latency Communications (Robotics, Factory Automation)***. Ultra-reliable low latency communications (URLLC) focus on mission critical services such as augment and virtual reality, tele-surgery and healthcare, intelligent transportation and industry automation. Traditionally over a wired connection, 5G offers a wireless equivalent to these extremely sensitive use cases. URLLC often requires the mobile core User Plane Function (UPF) to be located geographically closer to the end user in a Control and User plane Separation (CUPS) architecture to achieve the latency requirements.

- ***Massive IoT***. Massive IoT in 5G addresses the need to support billions of connections with a range of different services. IoT services range from device sensors requiring relatively low bandwidth to connected cars which require a similar service to a mobile handset. Network slicing provides a way for service providers to enable Network as a Service (NaaS) to enterprises; giving them the flexibility to manage their own devices and services on the 5G network.

- ***Enhanced Mobile broadband (eMBB)***. 5G Enhanced Mobile Broadband (eMBB) brings the promise of high speed and dense broadband to the subscriber. With gigabit speeds, 5G provides an alternative to traditional fixed line services. Fixed wireless access based on mmWave radio technologies enables the density to support high bandwidth services such as video over a 5G wireless connection. To support eMBB use cases, the mobile core must support the performance density, scalability, and security required.

[12] *See, e.g.,* "Private Networks," Small Cell Forum, *available at* https://www.smallcellforum.org/private-networks/; Press Release, "Qualcomm Technologies and Siemens set up the first 5G private standalone network in an industrial environment using the 3.7-3.8 GHz band," Qualcomm (Nov. 26, 2019), *available at* https://www.qualcomm.com/news/releases/2019/11/26/qualcomm-technologies-and-siemens-set-first-5g-private-standalone-network.

Of course, the 5G testbeds that the Department of Defense is establishing through the National Spectrum Consortium represent a prime opportunity to develop these use cases and determine the best options for network operation. Some deployments may require enterprise autonomy with an "own and operate" model. In other cases, mobile network operator services can best meet the use case requirements. Use case testbeds are ideal for answering the questions that arise in different deployment models regarding security, resiliency, agility, ability to execute on mission, and cost. The use cases that will be explored in these testbeds should help determine the various advantages and disadvantages of different radio technologies, including combinations of these different technologies.

More broadly, government agencies, especially DoD, should endeavor to be early deployers of these advanced networks. DoD's private LTE network experiments are a promising example.[13] As a large enterprise itself, the federal government can provide significant incentives for private sector investments and first mover innovations in these areas through steady funding streams for early stage deployment projects such as these. We urge the federal government to implement the National Strategy to Secure 5G in a manner that leverages these possibilities.

II. RIGOROUS TESTING OF SECURITY PERFORMANCE IN VARIOUS OPERATIONAL SCENARIOS IS CRUCIAL FOR PRACTICAL IMPLEMENTATION OF THE NATIONAL STRATEGY TO SECURE 5G

Security is a foundational aspect of Cisco's approach to 5G, and we commend the Administration for its recognition that the U.S. National 5G strategy must itself address security as a critical element. To that end, we highlight the five aspects of the foundational security fabric which deliver secure outcomes in the Cisco 5G network: (1) architecture and trust boundaries

[13] *See* Lopez, C. Todd, "DOD Announces New Locations for Additional 5G Testing, Experimentation," U.S. Department of Defense (June 3, 2020), *available at* https://www.defense.gov/Explore/News/Article/Article/2207390/dod-announces-new-locations-for-additional-5g-testing-experimentation/.

detailing the threat surface of 5G and IoT (both now and tomorrow); (2) technology trends and architectures impacting how the 5G network is secured; (3) visibility at scale; (4) threat and dark threat analysis; and (5) comprehensive threat mitigation. In the aggregate, we address the threat surface of today and tomorrow by providing the operator and consumer a level of service assurance for critical 5G based services.

These elements of Cisco's 5G security posture are valuable in addressing a key difference in 5G as compared to previous generations of mobile networks. Expansion of mobile computing power at the edge of the network—and the resulting blurring of the traditional notions of "core" and "edge"—changes the security landscape for 5G networks. First, there will be more threat surface because the devices at the edge will not necessarily need to push decision-making into the center or "core" of the network.

Instead, more data and metadata will be generated and consumed at the edge. This brings both challenges and benefits from a security standpoint. Attackers may leverage advanced persistent threats to infiltrate diffuse networks and then move laterally to cause damage, disrupt operations, or steal data. At the same time, the potential for significant improvements in security will result if industry can leverage the distributed nature of 5G networks to layer in visibility and control over the security of devices operating at the edge.

In turn, greater security capabilities are among the benefits that we expect to see from the adoption of technologies that boost speed, flexibility, and intelligence. These environments allow more options for how they are configured, deployed, and managed, which has the potential to increase the threat surface area and the opportunity for human error. However, trust security ("TrustSec") principles, such as zero-trust networking, segmentation, isolation, and least privileged access can be engineered into next generation wireless networks. The ability to move

more intelligence to the edge of the network along with advances in machine learning and artificial intelligence hold out hope for security that is capable of automation at scale—and, therefore, improved over current and legacy mobile networks.

Among the greatest unknowns as we move into a 5G powered world is precisely which capabilities will drive adoption and use. The boost of consumer speeds in 4G LTE led to broadband video services on mobile devices, but that result was not a predicted outcome in advance. Similarly, as discussed above, industrial and enterprise use of the new capabilities unlocked by 5G and Wi-Fi6 are likely and promising. But it is as of yet unclear which specific use cases made possible by these new capabilities will prove most impactful in the drive to unlock a new wave of American innovation and competitiveness. Without more knowledge about potential use cases, we may see incorrect assumptions driving decisions about how to architect and configure 5G networks—or we may see resulting uncertainty slow development and adoption of both 5G networks and innovations that could leverage their advanced capabilities.

This underscores the importance of the government investing in testbeds that will drive an understanding of potential use cases. Testbeds can also address key areas of operational security concerns, such as ensuring the security of the devices at the edge of the network that will be connected to 5G and managing non-technical and human/organizational risks that arise in certain use cases. With this in mind, Cisco recommends leveraging the testbeds and related U.S. government engagement with industry stakeholders to explore and experiment with the following elements of security:

- **Defense Uses vs. Commercial Uses.** 5G represents a potential step up in security from previous generations, but it has generally been created as a commercial grade system, not defense grade. For defense grade use cases, the government should determine whether additional security requirements are necessary, and if so, how best to implement them. Operational reliability and availability of the network in defense use cases, or other mission-critical use cases, may be different for commercial grade operations than what a

government agency or a critical infrastructure provider needs. This is not a new challenge; industry and the government (DoD in particular) have conducted such analyses in countless scenarios in the past, and these previous experiences should apply to 5G network security and data control as well.

- **Multi-Access Edge Computing (MEC).** MEC could be utilized as a security tool to isolate threats. Because MEC allows management of data at the edge, for some use cases, MEC could provide data sovereignty that may be important to military, intelligence, or other critical capabilities. However, MEC also means that instead of today's two-to-four exit points for the data on a provider network (e.g., in the case of VPN interconnectivity), 5G breaks the user plane from the control plane. For agencies like the Departments of State, Justice, Homeland Security and DoD that have numerous locations, this means exit points can be in the hundreds or even thousands in order for user data to stay local. This is attractive from a performance (e.g., latency) and data sovereignty perspective, but it necessitates that many exit points must be monitored and secured. More work is necessary to ascertain whether and how to effectively leverage and manage the costs and benefits of MEC capabilities.

- **Data Security and Privacy.** Encryption of data is generally required for 5G. But as a practical matter the standard for user data plane transmission rates is low, which tends to discourage the actual application of encryption technologies. Optionally, users can still deploy encryption at the application layer. Various use cases would illuminate the operational needs and challenges regarding encryption and data security and privacy that arise in different scenarios.

- **Identity Management.** Historically, there have been differences between identity management in enterprise settings as compared to service provider identity management. In an enterprise setting, the enterprise itself (specifically the IT department) controls identity management. When the user leaves the premise and becomes connected to a service provider, the enterprise can no longer directly manage security. TrustSec in the enterprise means the network can identify the user and apply policy to that user or administrative domain, such as micro-segmentation. However, as service providers move to software-defined networks, they will need to allow enterprise IT departments to apply their own identity management policies when users move on to the public network. As 5G identity management moves away from traditional radio space authentication to a certificate exchange method, the testbeds could further the development of identity management so that the enterprise can apply the same policies to the user's device no matter which public network platform is connecting the device. DoD has been at the forefront of defining hierarchies of trust policies, and the testbeds should build on that experience to advance 5G identity management.

In all cases, the DoD testbeds provide an immediate and meaningful first step for practical operational security testing. For additional steps beyond these testbeds, the Implementation Plan should leverage other formal government-industry collaborative mechanisms to take lessons

learned into other real-world deployments. These include outreach initiatives through the DHS National Risk Management Center ("NRMC"), applied technical research projects at the NIST National Cybersecurity Center of Excellence ("NCCoE"), and broader commercial and policy recommendations through the FCC's Communications Security, Reliability and Interoperability Council ("CSRIC").

III. THE NATIONAL STRATEGY TO SECURE 5G MUST BE IMPLEMENTED INTERNATIONALLY TO ENSURE THE DEVELOPMENT OF A DIVERSE GLOBAL ECOSYSTEM OF 5G EQUIPMENT AND SERVICES

In implementing its National Strategy to Secure 5G, the United States has an opportunity to demonstrate leadership for our partners in the international community—particularly defense allies, other free market democracies, and communications technology companies based in those countries—as it develops and deploys 5G networks and technology. Cisco believes that engaging with and encouraging international partners in the development of a diverse global ecosystem is the best way to protect U.S. economic and national security while simultaneously promoting responsible global development and deployment of 5G. Network security is a global issue, not merely a domestic one, and strategic engagements made by the U.S. government at the international level can inure to the benefit of American citizens, companies, and communities.

In particular, the Administration should continue to advance the Prague Proposals as an explicit part of implementing the National Strategy to Secure 5G.[14] There is global market strength among the 32 countries that have adopted the Prague Proposals, and that is why they focus on both technical and non-technical aspects of risk, including the rule of law, independent judicial oversight, corporate transparency and accountability, and security by design in 5G deployments.

[14] Prague 5G Security Conference, *The Prague Proposals* (May 3, 2019), *available at* https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

In a related initiative, the Center for Strategic and International Studies ("CSIS") organized a working group of industry experts, including from Cisco, to develop practical and concrete criteria for governments and network operators to use in assessing trustworthiness and security in implementing the Prague Proposals and the European Union's 5G Toolbox.[15] These initiatives provide an important conceptual and policy framework through which to guarantee a robust, competitive and diverse global market of trusted 5G equipment and services.

Finally, given the diversity of this global market and with the countless and as-yet-unknown use cases that 5G will enable, Cisco also encourages the Administration to think expansively about what the global 5G ecosystem actually is. As discussed above, 5G will enable dynamic and sophisticated new network capabilities—many of which have not yet been imagined, much less implemented. Yet, the precise use cases enabled will depend in some measure on decisions about network architecture and configuration.

Therefore, it is important that in implementing the National Strategy to Secure 5G the Administration not narrowly define 5G simply as a set of radio transmitter standards, but rather consider 5G broadly to encompass the entire network that contributes advanced wireless networking capabilities. Specifically, this broader vision should contemplate the use of unlicensed

[15] *See* Center for Strategic and International Studies, *Criteria for Security and Trust in Telecommunications Networks and Services* (May 13, 2020), *available at* https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services

spectrum by New Radio-Unlicensed and Wi-Fi.[16] 5G is not solely a service provider technology; instead, it is a highly flexible communications platform with different radios at the edge.[17]

If the advanced wireless networking market is limited to service provider offerings, the technologies available for use on their platforms will be governed exclusively by service provider purchasing cycles. The Administration should also recognize that enterprise and governments may stand up their own 5G network capabilities. For example, they may seek to operate their own "private 5G" networks in the CBRS band (or other bands).

A number of other jurisdictions are pursuing this course, including Germany and Japan, primarily with an eye on their manufacturing sectors. But the point is broader—any enterprise that wants to innovate its business process with 5G should have the ability to do so. The network owner may desire and should have the flexibility to choose between managing and operating such a private 5G deployment on its own or via a service provider. The National Strategy to Secure 5G should recognize and foster this broader view as it will draw more developers, manufacturers, integrators into the 5G market spurring a new wave of American innovation and competitiveness.

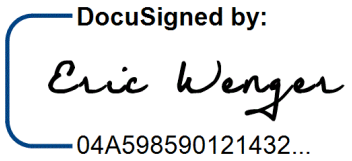
---

[16] Cisco is the largest manufacturer of Wi-Fi access points for use by enterprise customers globally. Wi-Fi is part of the 5G ecosystem as of 3GPP Release 15, and therefore will exist both as an alternative, stand-alone RAN but also as a 5G integrated RAN. Wi-Fi radio characteristics relative to 5G are similar such that the decision to use one radio endpoint instead of another should be driven by the use case requirements. In Cisco's view, the flexible integration, aggregation, and interworking of licensed and unlicensed networks, spectrum, and multi-connectivity will be critical as new 5G and IoT RATs are introduced in the industry. The integration of unlicensed network technologies such as Wi-Fi for use with conventional licensed cellular networks is now largely accepted as an essential ingredient of mobile network evolution. *See* "5G Networks: The Role of Wi-Fi and Unlicensed Technologies," Wireless Broadband Alliance (Sept. 6, 2017), *available at* https://wballiance.com/wp-content/uploads/2017/09/5G-Networks-Role-of-Wi-Fi-and-Unlicensed-Technologies-V2.pdf.

[17] There are many different approaches to license-exempt spectrum integration and aggregation. Some of them integrate and aggregate license-exempt networks at the core network level, while others integrate and aggregate license-exempt capabilities at the radio access network (RAN) level. For example, there is the trusted non-3GPP IP access interface, which uses a trusted wireless access gateway (TWAG) to integrate Wi-Fi into the 3GPP core network through the S2a interface to the packet data network gateway (P-GW). This is usually used for offloading 4G data traffic to Wi-Fi. Then there is the untrusted non-3GPP IP access approach, which uses an enhanced packet data gateway (ePDG) to integrate Wi-Fi into the 3GPP core network through the S2b interface to the P-GW. This is usually used to enhance indoor coverage through voice over Wi-Fi (VoWi-Fi). General discussion of these issues can be found at Wireless Broadband Association website, *available at* https://wballiance.com/wp-content/uploads/2019/09/RAN-Convergence-Paper-by-WBA-and-NGMN-Alliance.pdf.

CONCLUSION

Cisco is eager to partner with NTIA and others in government and industry to assist in implementing the National Strategy to Secure 5G. We urge the Administration to (1) promote agility, dynamism, and innovation through the development of new 5G use cases; (2) leverage testbeds for rigorous assessments of security performance in various operational scenarios; and (3) implement the National Strategy internationally to ensure the development of a diverse global ecosystem of 5G equipment and services.



Eric Wenger, Senior Director
Mary Brown, Senior Director

CISCO SYSTEMS, INC.
601 Pennsylvania Avenue, NW
9th Floor North
Washington, DC 20004
202.354.2948

June 25, 2020