Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Applicability of Section 4 of the Secure Networks	)	WC Docket No. 18-89
Act to the Rulemaking on Protecting Against	)	
National Security Threats to the	)	
Communications Supply Chain	)	

COMMENTS OF ERICSSON

Jared M. Carlson
Vice President
Government Affairs and Public Policy

Matthew Hussey
Director
Government Affairs and Public Policy

ERICSSON
1776 I Street, NW
Suite 240
Washington, D.C. 20006
Telephone: (202) 824-0114

May 20, 2020

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Applicability of Section 4 of the Secure Networks	)	WC Docket No. 18-89
Act to the Rulemaking on Protecting Against	)	
National Security Threats to the	)	
Communications Supply Chain	)	

COMMENTS OF ERICSSON

INTRODUCTION AND SUMMARY

Ericsson is a leading provider and trusted supplier of information and communications technology to service providers around the globe. The United States is our largest market worldwide, and we are committed to assisting the Commission in establishing an effective replacement program to ensure that all Americans can reap the benefits of secure, reliable connectivity and high-speed broadband.[1] The COVID-19 pandemic has drastically changed our daily lives and highlighted how essential connectivity is to our economy and workforce, students and teachers, and doctors and nurses. This stark reality underscores the importance of the Secure and Trusted Communications Networks Act of 2019 ("Secure Networks Act") to ensure the security and reliability of our networks and this proceeding to protect against national security threats to the communications supply chain. We have a clear appreciation for what is at stake and extensive experience in deploying networks – including equipment swaps with minimal service disruption and impact to consumers. We look forward to sharing our knowledge with the Commission and believe it can be very valuable to this proceeding.

[1] Public Notice, *Applicability of Section 4 of the Secure Networks Act to the Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, DA 20-406, WC Docket No. 18-89 (rel. Apr. 13, 2020) ("Public Notice").

A key element of Ericsson's global presence is its longstanding and expanding commitment to the United States. Our presence in the United States dates back nearly 120 years, and we now have 7,200 employees in the United States. As a trusted supplier for numerous domestic carriers, Ericsson has become the leader in North America with a 52 percent share of the Radio Access Network (RAN) equipment market.[2] Additionally:

- We have key development operations, as well as product, verification, and release activities, and our North American headquarters is located in Plano, Texas. We are actively expanding our investment in U.S. manufacturing and U.S. jobs, and we recently announced the first 5G smart factory in the United States, in Lewisville, Texas, which is now operational and producing radios for the U.S. market.

- Our Center of Excellence (CoE) in Lewisville is an enhanced tower technician training facility that provides best-in-class field services training and support for Ericsson's employees and partners. It will help facilitate the success of the replacement operations under development in this proceeding by contributing trained workforce to ensuring there are sufficient tower technicians to actually replace the equipment. In 2019, 847 tower tech trainees completed training at the CoE.

- We have supported 65 percent of the 5G deployments across the United States, including efforts to close the digital divide in rural America.

- We opened a 5G ASIC Design and Research & Development Center in Austin, Texas, to help accelerate 5G product development.

- We created a new innovation hub at Ericsson's Silicon Valley facility in Santa Clara, California, to enable our industry partners and customers to accelerate adoption of advances in artificial intelligence (AI) and machine learning. More broadly, we are committed to the U.S. 5G ecosystem.

- Our global sourcing of active components for our 5G radio base stations relies up to 90 percent on U.S. technology suppliers. And we maintain strategic partnerships with NVIDIA, Intel, Qualcomm, Juniper, and many other U.S. companies.[3]

[2] Dell'Oro Group, "Advanced Market Research Reports on Network Equipment Services," January 31, 2020, *available at* https://www.delloro.com/advanced-research-report/network-equipment-services/ ("Dell'Oro Group").

[3] *See* Prepared Testimony of Jason Boswell, Head of Security, Network Product Solutions, Ericsson North America, before the U.S. Senate Committee on Commerce, Science & Transportation, Hearing on "5G Supply Chain Security: Threats and Solutions," Mar. 4, 2020, *available at* https://www.commerce.senate.gov/services/files/45B9FF6F-280D-44BA-A29B-95B966F12A06.

Our customer base here in the U.S. is broad and diverse, ranging from nationwide providers to regional and rural providers as well. We are committed to working with our provider partners to extend wireless communications across the United States and to help bridge the digital divide. To that end, we have a Regional Carriers Customer Unit that is specifically structured to address the particular needs of the Tier 2 and Tier 3 operators we serve.

In these comments, we first describe our approach to equipment replacement, communications security, and open and interoperable standards. We then respond to key elements of the Public Notice:

- The Commission's role in implementing the Secure Networks Act should be to facilitate operators' replacement of untrusted equipment with secure equipment while avoiding picking winners and losers in the market.

- As the Commission engages in the statutory requirement to develop a list of "suggested replacements … or categories of replacements," it should identify categories of replacements available from any and all suppliers that have not been named "covered communications equipment and services," not a list of named suppliers or, even more concerning, precise names of equipment and services as "suggested" replacements.

- In order for this replacement process to promote innovation, the Commission's list of "categories of replacements" should be broadly inclusive of all options available on the market, including physical and virtual network equipment and services.

The goals of the Public Notice are critical and readily achievable. We look forward to engaging with all stakeholders toward that end.

DISCUSSION

I. ERICSSON'S BROAD EXPERIENCE IN NETWORK EQUIPMENT AND DEPLOYMENT OFFERS A STRONG FOUNDATION FOR REPLACING EQUIPMENT AND SERVICES WHILE MINIMIZING SERVICE DISRUPTION.

In North America, Ericsson leads with a 27 percent market share in mobile infrastructure services and, globally, excluding the Asia-Pacific region, Ericsson leads with a 30 percent market share.[4] Many of our existing customers may be eligible for replacement of non-Ericsson parts of their networks, and we are already working with certain operators to plan for this replacement process. Our Regional Carriers Customer Unit works with a diverse set of Tier 2 and Tier 3 operators that serve communities totaling 60 million users. We have established the Ericsson Regional Connect community to facilitate customer service to over 100 of our Tier 3 regional operators, supporting them with more than 450 support staff to enable regular communication and collaboration between the operators, to share best practices and case studies, and host in-person and virtual meetings to exchange information with key operator personnel.

We are very familiar with the needs of operators who intend to replace portions of their infrastructure under the Secure Networks Act, whether those components involve the antenna system, radio, RAN compute, mobile transport, or site system. Navigating the considerations involved in replacements (or swaps) requires close collaboration between operators and vendors. The following reflects several of the critical issues Ericsson has identified for determining the best course of action for planning and efficiently executing a swap:

- Operators' strong interest in minimizing consumer impact (even more important today given present public health circumstances) can lead to longer cycle time;
- Operators that typically self-perform incremental site updates will need vendor support to swap out their entire network; this can take significantly longer than a year – and the proposed six month extension – for operators with a large number of sites in very rural parts of America;
- Operators frequently have a mix of tower sites that are owned and leased, and where leased they are often shared with other operators and can require additional lead time for site acquisition updates, negotiations, and approvals;
- Most sites with multiple frequency bands and/or technologies must be migrated in a total and simultaneous manner, and such migration may require accommodations for additional tower space and structural improvements;

[4] Dell'Oro Group.

- In cases where microwave backhaul may be required to be changed, there are additional dependencies on process and scheduling if other customer traffic is being carried;
- Securing and retaining crews can be challenging when competing for limited resources in an environment with industry 5G modernization, mergers, and new entrant network upgrades; and
- Limited local tower crews can require mobilization of crews from other markets that leads to increased travel time and limit the work day.

In short, every swap scenario is different, but they are all complex undertakings.

Over the years we have developed three different swap methodology options based on the size of the operator and factors specific to the operator's network, each with differences in complexity, customer impact, and cost. We describe these methodologies below.[5]

First, in a site-by-site swap, we turn down an entire site while replacing network equipment. This is the least complex of our three methodologies, but it has the largest impact on an operator's consumers. The benefits of a site-by-site swap include faster replacement, lower labor costs, as well as lower infrastructure costs because existing facilities such as lines and power can be re-used. The disadvantages of a site-by-site swap include a larger customer impact and the need to have neighboring or overlapping coverage. The site-by-site swap is referred to as a "cold swap" because service from the site is down while removing the old equipment and installing the new equipment.

[5] *See also* "Ericsson Support Towards Protecting Against Threats to the Communications Supply Chain," at 15 (slide entitled "Swap Methodology Options"), attached to Letter from Jared M. Carlson, Ericsson, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Apr. 23, 2020) ("Ericsson Support Towards Protecting Against Threats to the Communications Supply Chain"), *available at* https://ecfsapi.fcc.gov/file/1042314506987/Ericsson%20April%2021%20Ex%20Parte.pdf.

Second, in a sector-by-sector swap, we turn down each sector of a site individually while replacing equipment in that particular sector.[6] This is a more complex methodology but has less of an impact on consumers than a cold swap.

Third, a parallel center of radiation ("RAD center") swap involves building a location for new equipment on the same tower on which the old equipment operates. This is the most complex of our swap methodologies, but it has the least impact on consumers. The benefits of a RAD center swap include minimal to no impact on the operator or consumer service.

II. ERICSSON'S GLOBAL LEADERSHIP IN COMMUNICATIONS SECURITY IS BUILT ON A PRINCIPLE THAT NETWORKS MUST, FROM THE OUTSET, BE TRUSTWORTHY, RESILIENT, AND SECURE BY DESIGN BASED ON RIGOROUS OPEN AND INTEROPERABLE SECURITY STANDARDS.

Ericsson takes a holistic approach to ensure that security is built into the network from the start, across the supply chain, software and hardware development, testing, implementation, and operation. For many years, Ericsson has worked systematically to incorporate "security by design" into all phases of product development, and we have a well-established internal governance framework for product security.

To secure and maintain the integrity of our supply chain, in all of our manufacturing and software development facilities worldwide, Ericsson relies on tight quality controls, traceability and integrity checks, regular site audits, tests, and verifications to ensure compliance with our own security standards and appropriate industry specification guidelines. All of Ericsson's software is verified, cryptographically signed, and distributed centrally from Sweden, and, when so required, under Swedish export licenses. We have strict software version controls with check-in/check-out security, meaning that both the Ericsson employee who wrote the code and the

[6] Sector antennas send out a pie-shaped wedge of radio frequency signals, typically between 30 degrees and 120 degrees wide. Multiple antennas (in the case of 120-degree sectors, three antennas) mounted on a structure can typically cover a wide area with better signal strength than an omnidirectional antenna might.

individual who reviewed/accepted the changes are logged. Binaries are provided via secure download from the Ericsson Software Gateway in Sweden, including a signature which provides a trust anchor that ensures the software originated from Ericsson and has not been tampered with in transit.

Standards work is a foundational component of good security assurance, as it ensures security and privacy requirements are met consistently across suppliers. Ericsson is a leader in developing the standards for 5G security (as it was for earlier generation wireless technologies). For instance, we participate in the global 3rd Generation Partnership Project (3GPP), and we are engaged in an effort through the Alliance for Telecommunications Industry Solutions (ATIS), supported by the Department of Defense, to develop standards for securing the 5G supply chain. In total, Ericsson is a member of more than 100 industry organizations, standards bodies, and other technology alliance groups. These standards are crucial for security because they give all suppliers and carriers a common – and open and transparent – technical understanding of interoperability and security, allowing for the vetting, identification, and correction of technical vulnerabilities. They also will allow new participants to compete with established global suppliers and ensure that the 5G ecosystem remains diverse and competitive.

In addition, Ericsson is a member of the O-RAN Alliance, which is advancing technical specifications for Open Radio Access Network ("Open RAN"). Ericsson serves as co-chair of two O-RAN Alliance working groups and as the editor of multiple technical specifications. Open RAN brings promising opportunities including RAN programmability, software/hardware disaggregation, and open interfaces to enable more flexibility. Open RAN may require adaptation for smaller operators (due to increased operational complexity among other issues), but as discussed in Section III.C below, the Commission's implementation of the Secure Networks Act should be technology neutral, neither prohibiting nor mandating its use.

Finally, once industry has developed and adopted standards, the next crucial step in security is effective network configuration and deployment. 5G is different from previous generations of wireless communications. Unlike the incremental steps from 1G to 2G to 3G to 4G, each of which constituted advances in both capability and security, 5G is a different type of network architecture. When fully realized, 5G will be "virtualized" across a service based architecture – meaning that the core network functions will happen through a cloud-based and "software defined" network, which allow tailored security solutions for each different network function, also known as a network "slice."

Virtualized networking will allow for unprecedented specialization in security – for instance, separating mission-critical network instances such as connected medical devices from less critical devices and functions. These new architectures and technologies will also facilitate more discrete control of access to data, topology obfuscation between network segments, greater requirements on inter-element encryption, provisions for extended authentication, enhanced privacy protections for subscribers, and many other new capabilities. Individual configurations in real-world deployments will be different in every case, but in all cases they should be based on the rigorous, open, and interoperable standards that Ericsson is helping develop now.

III. THE COMMISSION SHOULD IMPLEMENT THE SECURE NETWORKS ACT IN A MANNER THAT PROMOTES BOTH SECURITY AND INNOVATION.

The plain language of the Secure Networks Act affords the Commission wide flexibility to determine the optimal course to fulfill the statute's goals. We focus here on the issues surrounding the list of replacements, and the importance of moving forward with a list that provides for secure equipment and does not hinder innovation. In particular, the relevant passage includes an explicit choice regarding the type of list to develop:

> "The Commission shall develop a list of suggested replacements of both physical and virtual communications equipment, application and management software, and services ***or categories of replacements*** of both physical and virtual communications equipment, application and management software and services."[7]

This flexibility allows the Commission to facilitate operators' replacement decisions among the broad and diverse choices the market supplies for investment in secure equipment. It allows the Commission to avoid picking specific winners in the market.

At the outset, we note that Ericsson and other trusted suppliers in the market are eager to assist operators in navigating the swap choices that they have before them and in replacing equipment from "covered" entities. Ericsson offers virtualized and software upgradeable solutions that will render future maintenance and modernization more affordable than their present equipment. This is a promising moment for both innovation and security in U.S. communications networks, and the Commission's implementation of the Secure Networks Act can provide a significant advance in both areas. To this end, below we respond to the three questions from the Public Notice that we believe are core to the effectiveness of the Commission's actions:

(1) *How should the Commission develop a list of suggested replacement communications equipment and services?*

(2) *Can the list simply include all equipment and services from certain companies, or must it include the precise names of the equipment and services from those companies that are eligible for reimbursement?*

(3) *Should this list include suppliers of virtual network equipment and services?*[8]

[7] Section 4(d)(1), Pub. L. 116-124, 133 Stat. 158 (2020) (emphasis added).

[8] Public Notice at 4.

A. The Commission Should Develop a Reference List of General "Categories of Replacements of Both Physical and Virtual Communications Equipment, Application and Management Software and Services."

The Secure Networks Act provides the Commission the option of developing a list of "categories of replacements," and the Commission should take this approach rather than naming specific "suggested" suppliers (or, as discussed further below, particular models of equipment). All companies that are not designated as "covered communications equipment or services" on the list required by Section 2(a) of the Secure Networks Act should be presumed under the law to be eligible to provide replacement equipment and services. The Commission should not develop yet another list of "suggested" companies on top of this separately required list of "covered" entities, which the Commission separately is designating. The Commission should refrain from taking the unprecedented step of developing a Commission-preferred list of "suggested" private suppliers chosen from among perhaps hundreds of options in this innovative, diverse market, as such a list would constitute a soft mandate to operators.

The Commission's development of a list of "suggested" suppliers poses other risks as well. For instance, such a list could diverge from approaches taken by other agencies with relevant expertise, potentially causing regulatory uncertainty and confusion in the market. It could also impact the federal procurement arena, and affect operator decisions outside the universal service setting. The Commission therefore should not develop such a list, particularly as the statute provides the flexibility for the Commission to develop a list of "categories of replacement."

B. The Commission's List of "Categories of Replacements" Should Include All Pertinent Equipment and Services Available, Rather than a List of Precise Names of Equipment and Services.

The Commission should provide a high-level guide of equipment and service categories that is broadly inclusive of all general types of equipment and services to be replaced, including, as required by the Secure Networks Act, "both physical ***and*** virtual communications equipment, application and management software and services."[9] The Commission can develop this list based on the knowledge it gains from its ongoing information collection under this proceeding regarding the existence and types of "covered communications equipment and services" that will be replaced. The list can then serve as a reference for operators who are determining how best to pivot from "covered" suppliers to a longer-term future of innovative and secure networks.

Just as the Commission should refrain from developing a list of specific "suggested" suppliers, it should also not list precise pieces of equipment or names of equipment and services. Even in this relatively narrow context of one-time reimbursable replacement of equipment and services from "covered" entities, such a list would constitute a command-and-control style government preference that would repress a dynamic and diverse market that presently has an opportunity through the forthcoming replacement process to make major advances in the innovation and security of U.S. communications infrastructure. Such an approach could not only stifle innovation but effectively bind carriers to the Commission's stated choices.

C. The Commission's List of "Categories of Replacements" Should be Broadly Inclusive of the Offerings of Suppliers of Virtual Network Equipment and Services.

As described above, virtualized network equipment and services are increasingly a significant part of the future of secure, reliable communications. Ericsson's dual-mode 5G Cloud Core illustrates the value and importance of such equipment as a replacement option, as it allows operators to simultaneously support both 4G LTE and 5G, leverages software containers and microservice architecture to be completely platform agnostic, and can be run on an

[9] Section 4(d)(1), Pub. L. 116-124, 133 Stat. 158 (2020) (emphasis added).

operator's private cloud computing architecture or a public cloud.[10] Ericsson and other trusted suppliers in the diverse, competitive U.S. market for communications equipment and services have developed virtual network innovations that should neither be excluded nor mandated through the Commission's implementation of the Secure Networks Act.

CONCLUSION

Ericsson appreciates the difficult task ahead for the Commission. Our technical experts are available to aid the Commission as it considers the myriad issues associated with assisting U.S. operators with the replacement of equipment from companies deemed to pose a heightened national security risk.

/s/ Jared M. Carlson
Jared M. Carlson
Vice President
Government Affairs and Public Policy

Matthew Hussey
Director
Government Affairs and Public Policy

ERICSSON
1776 I Street, NW
Suite 240
Washington, D.C. 20006
Telephone: (202) 824-0114

May 20, 2020

[10] *See* Ericsson Support Towards Protecting Against Threats to the Communications Supply Chain at 24-25.