Testimony of Jason S. Boswell
Head of Security
Network Product Solutions
Ericsson North America

on
"5G Supply Chain Security:
Threats and Solutions"

Before the
U.S. Senate Committee on Commerce, Science & Transportation

March 4, 2020

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to appear today on behalf of Ericsson and to share our views on the important subject of supply chain security in the 5G world. Ericsson commends the Committee for its focus on these important issues, and we welcome the recent passage of Chairman Wicker's bipartisan Secure and Trusted Communications Networks Act. As Head of Security for Network Product Solutions in Ericsson North America, I advise Ericsson's technicians, engineers, partners, and customers on creating and maintaining secure Ericsson solutions across the country. I also represent Ericsson in numerous industry initiatives and collaborative efforts with government to develop and implement industry-wide practices and policies to make the 5G supply chain trustworthy, resilient, and secure. Since my early days as an engineer more than 20 years ago, I have spent the entirety of my career focused on security and advanced telecommunications. I am pleased to be able to describe Ericsson's perspective on the important topic of securing 5G and its supply chain.

I. Introduction

A Pivotal Moment for 5G. 5G will accelerate innovation, enhance productivity, and make our lives better through transformative use cases in manufacturing, telemedicine, agriculture, connected cars, smart cities, and the Internet of Things, to name a few, plus a host of applications and services that are still to come. 5G will deliver significant benefits to consumers and business alike.

But this innovation brings new security challenges for the mobile ecosystem as well, with broader attack surfaces, more devices, and greater traffic. The United States is expected to account for 50 percent of the data breached or compromised across the globe by 2023 – we

will be the lead target for cyberattacks. This is a clear call to action for the U.S. We need networks that are trustworthy, resilient, and secure by design – all on day one.

In short, as we embark on the 5G future and usher in the next decade of telecommunications, we face a series of critical decisions, and we have an opportunity for the U.S. to set a global example in 5G network security across policy, technology, and standards. Whether we live up to this moment will depend on how industry and government together answer these questions:

- Will 5G be innovative and dynamic?
- Will 5G be secure and reliable?
- Will 5G support the rule of law and enable fair competition and the robust marketplace necessary to protect national security?

I believe that with intentionality and foresight, the United States will provide an emphatic "yes" in response to each of these questions. This morning, I will share Ericsson's perspective on key priorities and key action items that will help guide us through this moment.

Ericsson: Who We Are and What We Do. At Ericsson, we long ago embraced the idea of making communications available for everyone, and we have aggressively executed on that vision ever since. Today, we serve customers in the United States and more than 180 other countries.

Ericsson is a global 5G leader. To highlight just a few accomplishments:

- We were the first supplier with commercial 5G live networks in four continents, and currently we support twenty-four live 5G networks in fourteen countries.
- We now support the widest ecosystem of supported devices on 5G live networks, with over forty.

- In every nation state that has conducted a national security 5G assessment, Ericsson has been designated as both a secure and trusted 5G supplier.

- Since 2015, we have delivered more than five million 5G-ready radio units world-wide, which only need a remote software update to launch 5G; hypothetically, this number of radios corresponds to covering the entire U.S. and Europe with 5G.

- We led the way on 5G standards, with the highest share of 5G essential patent declarations – 15.8 percent – of any organization in the world. And more broadly, we have one of the industry's strongest intellectual property portfolios, which includes more than 54,000 granted patents worldwide. Ericsson is the largest holder of standard essential patents for mobile communication. Our unrivalled patent portfolio covers 2G, 3G, and 4G, and we are the main driver of industry standardization for 5G.

Our primary headquarters is in Sweden – a country with which the U.S. has a longstanding defense cooperation – but we have key development operations, as well as product, verification, and release activities, in North America. The United States is our largest market, and Ericsson has a longstanding and expanding commitment to the U.S. Our presence in the U.S. dates back nearly 120 years. Ericsson now has over 7,000 employees working in the U.S., and our North America headquarters is located in Plano, Texas. And, we are actively expanding our investment in U.S. manufacturing and U.S. jobs. Of note, we are opening our first 5G smart factory in the United States, in Lewisville, Texas. This facility will be a connected smart factory, producing Advanced Antenna System radios to enable rapid 5G deployments. In addition, our Lewisville, Texas Center of Excellence (CoE) is an enhanced tower technician training facility that provides best-in-class field services training and support for Ericsson's employees and partners. In 2019, 847 tower tech trainees completed training at the Lewisville CoE.

Over the last two years, Ericsson has had other investments and achievements in the United States, including:

- Producing the first 5G radios in the U.S. in 2018, with a production partner in St. Petersburg, Florida;
- Supporting 65 percent of the 5G deployments across the United States, including efforts to close the digital divide in rural America;
- Opening a 5G ASIC Design Center in Austin, Texas, to help accelerate 5G product development; and
- Creating 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.

Apart from its direct investments in the U.S., Ericsson serves a broad and diverse U.S. customer base, which includes nationwide and regional communication service providers serving both rural and urban markets with all technologies (wireline and wireless telecommunications, cable, and satellite). We have partnerships and collaborations with rural Wireless Internet Service Providers (WISPs) and carriers – such as GCI Communications, Cellcom, Bluegrass Cellular, and many more – in furtherance of our commitment to bring 5G to rural areas. Ericsson also maintains strategic partnerships with NVIDIA, Intel, Qualcomm, Juniper, and many other U.S. companies. In fact, Ericsson's global sourcing of active components for Ericsson's 5G radio base stations relies up to 90 percent on U.S. technology suppliers. Finally, we participate in more than 100 industry organizations, standards bodies, and other technology alliance groups.

As discussed further below, Ericsson employs a holistic approach to ensuring the security of its supply chain and its products, which is made more effective by an environment here in the U.S. consisting of pro-deployment public policies and 5G investment, combined with industry-led collaboration with government for a secure 5G ecosystem.

II. Ericsson's View of the Priorities That Enable a Successful and Secure 5G Rollout

Security is inextricably tied to the successful development of 5G networks – without one, you simply do not have the other. Before explaining Ericsson's approach to assuring 5G supply chain security, let me identify three key priorities for enabling a successful and secure 5G rollout.

Accelerating 5G deployment in North America. The United States enjoyed first mover advantage in the 4G world, and it can win the 5G pole position as well. Indeed, the North American market is large enough to lead the world market, setting the global agenda for innovation and security and market competition. Conversely, any delay in 5G advancement policies could allow other actors that may pose national security risks to gain the first-mover advantage in the 5G investment cycle and set technology standards for global companies to adopt. In short, being first in 5G deployment is not merely an honorarium – it is a meaningful step toward a secure 5G ecosystem.

As Ericsson has advocated, and as the members of this Committee have advanced, Congress can accelerate 5G deployment in the U.S. by taking the following near-term actions:

- Increase spectrum availability, especially mid-band;
- Put in place reasonable, streamlined small cell siting rules;
- Develop and deploy a skilled tower workforce; and
- Ensure effective incentives to encourage 5G deployment in rural areas.

Below, I identify several measures before the Senate that can help accomplish these objectives.

Strengthening and ensuring the long-term viability of a competitive, dynamic, diverse, robust global market of trusted and secure suppliers. Over the past two decades, the global

market of wireless communications equipment suppliers has seen significant consolidation, but today there are a number of suppliers of 5G radio access network equipment in addition to Ericsson. Additional suppliers, including U.S. companies, provide different elements of core network equipment, and evolving innovations in open and interoperable networking and virtualization will allow new participants to compete with established global suppliers. In short, even with bans on Chinese vendors, the 5G ecosystem presently is diverse and competitive – attributes that are imperative not only for ever-advancing innovation but also to ensure security and resiliency throughout global networks.

A key strategic goal for public policy aimed at a secure and trusted 5G supply chain is to maintain a global, competitive, diverse market of trusted suppliers. Network security is a global issue, not just a domestic one, and security on a global level only reinforces and enhances security here at home. We should therefore continue to encourage the adoption, without delay, of principles and guidelines favoring trusted suppliers and supply chains – on a *global* basis. We all have a mutual interest in such a competitive market – suppliers and service providers alike. And we agree with the principles that security and trust are two independent factors that need to be assessed to protect 5G networks. These principles are key to establishing an end-to-end view of risk across the multiple layers of telecommunications infrastructure.

Supporting the important, ongoing work of standards processes and government-industry coordination. Ericsson is a leading participant in developing the standards for 5G security through 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. These technical standards are crucial for security because they give all suppliers and carriers a common – and open and transparent – technical understanding of interoperability and security. This allows for vetting and identification and correction of technical vulnerabilities. To be clear, 5G security standards and 5G supply chain standards are presently still under development, and Ericsson is helping shape them for long-term security.

Once industry adopts standards, the next crucial step is effective network configuration and deployment. Here, I need to emphasize how 5G is different from previous generations of wireless communications. Unlike the steps from 1G to 2G to 3G to 4G, each of which constituted advances in both capability and security, 5G is a totally new and different technology and network architecture. When fully deployed, 5G will be "virtualized" across a service based architecture (SBA) – 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 capabilities for specialization in security for different isolated functions – 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 allow for 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.

We believe the role of the government in advancing the security of these deployments is to continue to put its attention and resources behind the robust government-industry collaboration efforts that are presently underway. In short, we must work together effectively and efficiently to ensure that these deployments are secure, as described below.

III. Ericsson's Activities and Leadership That Advance These Priorities

Security is a top priority for Ericsson, and our actions on security reflect our philosophy: Networks must, from the very start, be trustworthy, resilient, and secure by design.

How does Ericsson ensure a secure supply chain? In all of our manufacturing and software development facilities globally, 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 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.

Where are Ericsson products developed and manufactured? Ericsson has a global, flexible, high-integrity supply chain, with manufacturing established in several countries around

the world – including a sizeable presence in the U.S., as I described above. Since 2018, we have been proactively executing a regionalization strategy for our supply chain, to place manufacturing and development as close to the customer market as possible in order to mitigate potential risks or regional disruptions and reduce dependence on one supply site or vendor. In general, all active "intelligent" 3PP electronics (*e.g.*, digital semiconductors, silicon-based technology, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), etc.) for the Ericsson Radio System (ERS) are predominantly sourced from U.S. companies, with a minor part from Japanese, Korean, and European companies.

How does Ericsson provide security assurance? Ericsson takes a holistic approach to ensure that security is built in from the start, across supply chain, software and hardware development, testing, implementation, and operation. For many years, Ericsson has worked systematically to incorporate security from the start (security by design) into all phases of product development, and we have a well-established internal governance framework for product security. This framework is how Ericsson is able to consistently deliver on our product security commitment. The framework's key characteristics include:

- Defining our product security and privacy ambition level;
- Ensuring the implementation of appropriate security and privacy;
- Following up and measuring actual product security and privacy status; and
- Enabling professional security services, such as security and privacy training recommendations, solution level integration guidance, and potential hardening activities that need to be included in customer delivery projects.

In addition, all personnel and suppliers follow Ericsson's Code of Conduct and Code of Business Ethics. Ericsson places top priority on protecting our customers' networks and their customers'

data, as well as our intellectual property, all of which are governed under internal policies, and certified by ISO/IEC 27001 and ISO 9001, which are recognized as international guidelines on Information Security Management and requirements for Quality Management Systems, respectively.

Finally, we strongly believe in the principles of responsible vulnerability disclosure towards all parties involved. Accordingly, the Ericsson PSIRT (Product Security Incident Response Team) is responsible for our product vulnerability management process, coordination of customer product security incidents, and reported security issues affecting Ericsson products, solutions, and services.

How does Ericsson promote and advise on industry-wide best practices in 5G and supply chain security? Our security efforts do not end with our products – Ericsson actively contributes to a number of U.S.-based industry initiatives organized around ensuring supply chain security. These include the Communications Sector Coordinating Council (CSCC) and its Cybersecurity Committee (where I participate directly as a member), the Council to Secure the Digital Economy (CSDE), and multiple working groups within the standard-setting organization ATIS.

I also personally provide leadership in numerous government-industry initiatives convened to promote collaboration on supply chain security. I will cite three examples here, which are especially relevant to this discussion.

First, it has been my privilege to participate in the groundbreaking work of the Department of Homeland Security (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management Task Force. The DHS ICT Supply Chain Risk Management Task

Force exemplifies how industry and government collaboration can quickly and effectively deliver useful, sharable, expert-driven guidance in complex areas like supply chain and 5G security. The Task Force represents a formal, action-oriented collaboration between industry and government that ties together various streams of activity. For example, in September 2019, the Task Force released an interim report with findings and recommendations from working groups that focused on:

- The timely sharing of actionable information about supply chain risks across the community (WG1);
- The understanding and evaluation of supply chain threats (WG2);
- The identification of criteria, processes and structures for establishing Qualified Bidder Lists (QBL) and Qualified Manufacturer Lists (QML) (WG3); and
- Policy recommendations for incentivizing the purchase of ICT from original equipment manufacturers and authorized resellers only (WG4).

In 2020, I will continue Ericsson's work in the Task Force Threat Evaluation Working Group (WG2) by analyzing mitigations and risk determination across multiple areas of the supply chain and making recommendations on best practices and methodologies. I will also be co-chairing a new working group (2020 WG4) to develop attestation frameworks around various aspects of supply chain risk management. This will help make requirements such as the NIST security standards and other risk guidelines more understandable, predictable, and useful, and also will address gaps in risk management or visibility by providing a flexible template that can help guide planning and assessments and provide clarity for acquisition reporting and vetting processes.

Second, I participate in the important work of the President's National Security Telecommunication Advisory Council (NSTAC). In particular, I serve on a subcommittee tasked

by the NSTAC with examining the security impact of software-defined networking (SDN) on the U.S. government's National Security and Emergency Preparedness functions, identifying the challenges and opportunities provided by SDN, and assessing the use of SDN and other virtualization technologies in support of national security.

Third, I represent Ericsson on the Communications Security, Reliability, and Interoperability Council (CSRIC), which makes security policy recommendations to the Federal Communications Commission (FCC). Ericsson is working across three working groups in the current iteration of CSRIC, CSRIC VII, notably:

- Managing Security Risk in the Transition to 5G (WG2), in which I am directly involved;
- Managing Security Risk in Emerging 5G Implementations (WG3); and
- 911 Security Vulnerabilities during the IP Transition (WG4).

Beyond these activities, we also work closely with other government departments and agencies, including the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST), both within the Department of Commerce, as well as with the Departments of Defense and Energy.

Standards work is another foundational component of good security assurance, as it supplies guidance and frameworks that ensure security and privacy requirements are met consistently. Ericsson has been a leading contributor in standards and frameworks groups such as 3GPP, ETSI, IETF, GSMA, IEEE, the O-RAN Alliance, the Open Network Foundation, and many more. As noted above, in total, Ericsson is a member of more than 100 industry organizations, standards bodies, and other technology alliance groups, as part of our mission to drive 5G forward.

IV. Ericsson's Recommendations for the Committee to Support and Promote These Priorities

At the beginning of my testimony, I listed three questions that mark this moment in the trajectory to 5G:

- Will 5G be innovative and dynamic?
- Will 5G be secure and reliable?
- Will 5G support the rule of law and enable fair competition and the robust marketplace necessary to protect national security?

As noted above, I believe that with intentionality and foresight, the answer to these questions can be an emphatic "yes." Now for the hard part: How do we get there?

As a general matter, Ericsson urges the Committee to support the various efforts described above, with an eye toward ensuring that industry and government are coordinating efficiently and collaborating productively on 5G security and supply chain matters, both domestically and globally.

More specifically, we recommend that the Committee take the following steps:

(1) ***Pass, implement, and oversee 5G security legislation.*** As I noted at the outset, the Senate's recent passage of Chairman Wicker's Secure and Trusted Communications Networks Act represents a thoughtful and crucial step forward. We look forward to the President signing this bill and stand ready to work with the small operators who will have to replace existing equipment. As the Committee is well aware, further opportunities to build on the momentum of that legislation await, as several additional bipartisan 5G security-related bills have passed in the House of Representatives. These include the House companion bill to Senator Cornyn's Secure 5G and Beyond Act, co-sponsored by Senators Sullivan and Blackburn of this Committee and others, which would require the U.S. to develop a 5G security strategy. Passage of such

measures in the Senate would help demonstrate the U.S. commitment to 5G security to countries around the world grappling with these issues.

(2) ***Support actions to accelerate 5G deployment.*** As I discussed, Ericsson believes that accelerated U.S. 5G deployment will in turn protect the security of the 5G supply chain, a goal that can be achieved through (i) increasing spectrum availability, especially mid-band; (ii) putting in place reasonable, streamlined small cell siting rules; (iii) developing and deploying a skilled tower workforce; and (iv) ensuring effective incentives to encourage 5G deployment in rural areas. We commend the work being done in these areas and urge the Committee to take up proposals to advance 5G deployments in the U.S., such as the STREAMLINE Act introduced by Senators Thune and Schatz, which would preempt certain state/local small cell deployment regulation; the TOWER Infrastructure Deployment Act introduced by Senators Gardner and Sinema, which would require the FCC to set up an Advisory Council to look at tower workforce issues; and the Telecommunications Skilled Workforce Act recently introduced by Senators Thune, Tester, Moran, Peters, and Wicker, which would require cooperation among various agency heads to develop recommendations and guidance that would empower the U.S. to catch up on the workforce demands of the 5G era.

(3) ***Continue to enable a secure and robust marketplace of trusted suppliers in the U.S. and globally.*** As I have discussed, one of the key priorities for 5G is to strengthen and ensure the viability of a competitive, dynamic, diverse, and robust marketplace of trusted and secure suppliers on a global level, much like what we already have in the United States, recognizing that global and domestic security are intertwined. Such a marketplace, involving trusted and secure companies like Ericsson, can counter other potential players that may pose threats to

national security. The Committee should remain attentive to factors that might promote – or undermine – the development of this global marketplace.

(4) ***Continue to hold hearings on the subject of 5G security.*** In Ericsson's view, hearings such as this one provide an important vehicle for highlighting what industry is doing to ensure a secure 5G world – and for maintaining pressure on industry to stay true to its security commitments. Such hearings can have a similar motivating impact on government actors with security responsibility within their respective jurisdictions around the world. Shining additional light on all of these efforts will make them more effective in ensuring a secure supply chain.

* * *

On behalf of Ericsson, I thank the Committee for its leadership in this area. We look forward to continuing to work with you, other government actors, and our industry partners to ensure that the 5G world is a secure one. Thank you again for the opportunity to testify today, and I look forward to your questions.