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

on
"A Safe Wireless Future:
Securing our Networks and Supply Chains"

before the
U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Communications and Technology

June 30, 2021

ERICSSON

Chairman Doyle, Ranking Member Latta, Chairman Pallone, and Ranking Member McMorris Rodgers, Members of the Committee, thank you for the opportunity to appear today to share Ericsson's views on the future of secure and reliable wireless communications. We appreciate your ongoing focus on secure communications networks—a matter of top priority to Ericsson and of critical importance to our nation.

Ericsson has focused on network security for decades, contributing to numerous technical committees and standards bodies, and establishing dedicated internal security organizations. As Head of Security for Network Product Solutions in Ericsson North America, I advise Ericsson's technicians, engineers, partners, and customers on secure Ericsson solutions. I also represent Ericsson in numerous industry initiatives and collaborative efforts with government, including the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Security Information Exchange (NSIE), on the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC), on the Department of Homeland Security's (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, as well as many other working groups and committees.

The last time I had the honor to testify before Congress was March 4, 2020, and in the ensuing 15 months, our society has learned the indispensable value of secure, reliable, remote connectivity in virtually every aspect of our lives, from education to business to social activities. I know from my work at Ericsson – and from my service on NSTAC and other bodies – that the ICT industry as a whole has stepped up and excelled during this historic challenge.

The ICT industry is using a model of private sector leadership facilitated by coordinated government partnership. As part of NSTAC, during the past year I co-authored two reports to the President on (1) ICT resiliency during COVID-19 and recommended steps that the Administration should take to ensure the resiliency of U.S. national security and emergency preparedness (NS/EP) communications and (2) a long-term look-ahead to communications security and reliability demands of the future. In these reports, and in other collaborative efforts, experts across the ICT industry have coalesced around three core goals to protecting the nation's critical infrastructure:

1. Secure the communication itself, end to end;
2. Ensure the resilience of the network; and
3. Protect the integrity of the network supply chain.

These pillars are important whether we're talking about 3G, 4G, 5G, Wi-Fi, cloud environments, or wireline infrastructure. The thoughts I share with you today derive from this work.

Above all else, I want to emphasize that we are in a pivotal moment for the future of secure, reliable wireless communications. We must not lose focus.

5G will accelerate innovation and deliver transformative benefits by enabling greater connectivity, lower latency, enhanced capacity, and more sophisticated network management. While this increased connectivity poses new security challenges for the mobile ecosystem, with broader attack surfaces, more devices, and greater traffic, the capabilities enabled by 5G and security features built into the standards for 5G architecture are poised to make 5G networks the most secure yet.

We do expect the United States to be the lead target for cyberattacks in the coming years – a clear call to action for all of us. We need networks that are trustworthy, resilient, and secure by design. We are at a fork in the road, and we have an opportunity for the U.S. to set a global example in 5G network security across policy, technology, and standards. Will the 5G world be innovative and dynamic? Secure and reliable? Will it enable fair competition and a robust marketplace necessary to protect national security? I believe that with intentionality and foresight, the United States will answer "yes" to each of these questions.

I want to share Ericsson's perspective on key priorities and key action items that will help guide us through this moment.

Ericsson serves customers in the U.S. and in more than 180 other countries, with over 100,000 employees worldwide – nearly 8,000 of whom are based in the U.S., at our headquarters in Plano, Texas. Although our global headquarters is in Sweden, a long-time U.S. partner and party to a formal cooperative defense agreement, the U.S. is effectively our "domestic" market, as it is our largest market, providing over one-third of Ericsson's global revenue, and it is also the market that drives our global R&D investments. Ericsson has a longstanding and growing commitment to the United States. Our presence in the U.S. dates back nearly 120 years and we have key development operations, as well as product, verification, and release activities, in North America. Ericsson also maintains strategic partnerships with NVIDIA, Intel, Qualcomm, Juniper, and many other U.S. companies. In fact, all third party active "intelligent" 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.

We are actively expanding our investment in U.S. manufacturing and U.S. jobs. Last year we opened a $100 million 5G smart factory in Lewisville, Texas, where we are building Advanced Antenna System radios to enable rapid 5G deployments. We have four R&D locations in the US. We were the first vendor to launch 5G with all Tier-1 service providers in the U.S., and we are committed to helping to close the digital divide in rural America. Ericsson is also a global 5G leader. We led the way on 5G standards, with the highest share of 5G patent declarations – approximately 16.1 percent of essential 5G patent families – of any organization in the world.[1] More broadly, we are the largest holder of standard-essential patents for mobile communications, with 57,000 patents. Finally, we participate in more than 100 industry organizations, standards bodies, and other technology alliance groups.

Security is inextricably tied to the successful development and deployment of 5G networks, and we see three key priorities for enabling a successful and secure 5G rollout:

First, accelerating 5G deployment in the United States through increasing spectrum availability, especially mid-band spectrum; putting in place reasonable, streamlined small cell siting rules; and ensuring effective incentives to encourage 5G deployment in rural areas. This will give the U.S. the first mover advantage in 5G that it enjoyed in 4G – a meaningful step toward secure 5G. It will also ensure that the U.S. benefits from the extensive economic benefits that will come with 5G leadership, including an additional 4.5 million jobs and $1.5

[1] Christina Petersson, *When it comes to 5G patents, quality and essentiality matters* (Nov. 12, 2020), https://www.ericsson.com/en/blog/2020/11/5g-patents-quality-essentiality.

trillion in economic growth.[2] To that end, wireless and 5G infrastructure should play a prominent role in any government broadband programs, and should be funded in any broadband infrastructure funding legislation to ensure that rural areas are not left behind when it comes to 5G benefits, including mobility.

Second, strengthening and ensuring the long-term viability of a competitive, diverse global market of trusted and secure suppliers. Diversity in the network avoids "single point of failure" problems and also limits espionage and sabotage vulnerabilities. We all have a mutual interest in a diverse market – suppliers and service providers alike. U.S. Secretary of State Tony Blinken articulated the value of leveraging these strategic co-dependencies for the good of the U.S. and our partners and allies when addressing NATO earlier this year:

> We should bring together tech companies from countries like Sweden, Finland, South Korea, the United States, and use public and private investment to foster a secure and trustworthy alternative. We've spent decades developing relationships with countries that share our values in every part of the globe. This is why we invested so much in these partnerships – so we can come together in innovative ways to solve new challenges like these.[3]

To this end, the U.S. government should foster a diverse global market of trusted suppliers that are committed to delivering high performing, secure, and energy efficient network products to U.S. operators.

Third, supporting the important, ongoing work of standards processes and government-industry coordination. Ericsson is a leader in developing the standards for 5G security through the global 3rd Generation Partnership Project (3GPP), and we are engaged in

[2] Boston Consulting Group (BCG), *5G Promises Massive Job and GDP Growth in the US* (Feb. 2, 2021), *available at* https://www.ctia.org/news/report-5g-promises-massive-job-and-gdp-growth-in-the-u-s.
[3] Hon. Antony J. Blinken, Secretary of State, "Reaffirming and Reimagining America's Alliances," NATO Headquarters Agora (Mar. 24, 2021), https://www.state.gov/reaffirming-and-reimagining-americas-alliances/.

an effort through the Alliance for Telecommunications Industry Solutions (ATIS), supported by the Department of Defense (DoD), to develop standards for securing the 5G supply chain. We also serve on the O-RAN Alliance's Security Focus Group, which is in the early stages of developing Open RAN security specifications. These technical standards are crucial for security because they give all suppliers and carriers an open and transparent opportunity to identify and correct technical vulnerabilities, leading to effective network configuration and deployment. 5G is different from previous generations of wireless communications. Unlike the advances from 1G to 2G to 3G to 4G, 5G is a totally new and different technology and network architecture. 5G network functions will operate through a "virtualized" cloud-based network, allowing tailored security solutions for each different network function that will provide unprecedented capabilities for specialization in security for different isolated critical functions, for example, separating connected medical devices from less critical devices. These configurations in real-world deployments will be different in every case, but they should always be based on the rigorous, open and interoperable standards that Ericsson is helping to develop, and they should be bolstered by ongoing government-industry coordination efforts, such as the work of the FCC's CSRIC and the communications security initiatives that are underway through the leadership of the National Telecommunications and Information Administration (NTIA).

Ericsson commits significant resources to reach these goals. In short, we ensure that networks must, from the very start, be trustworthy, resilient, and secure by design.

First, in all of our manufacturing and software development facilities globally, Ericsson secures our own supply chain with tight quality controls, traceability and integrity checks, regular site audits, tests, and verifications. Additionally, in 2018 – prior to the disruptions

caused by the pandemic – we began 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. Particularly following the sophisticated compromise of SolarWinds' software supply chain, I want to emphasize Ericsson's approach to developing secure solutions. Well before the cyber attack on SolarWinds last year, all of our software was scanned, verified, cryptographically signed, and centrally distributed. We have strict software version control with check-in/check-out security, meaning that both the Ericsson employee who wrote the code and the individual who reviewed and accepted the changes are logged.

Ericsson supports the goals espoused in the President's Executive Order on Improving the Nation's Cybersecurity, which defines the term "Software Bill of Materials" or "SBOM" as a "formal record containing the details and supply chain relationships of various components used in building software."[4] Ericsson has vast experience in secure software development, through industry best practices such as the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF), which serves as one of our models for securely using proprietary, third-party, and open source software in development projects. As part of this process, Ericsson maintains internal SBOMs for its products and makes these available through a secure portal to customers on a contractual basis, protecting the confidentiality and authenticity of this important information. Furthermore, Ericsson evaluates its own software to identify vulnerabilities, utilizing static and dynamic code testing, privacy

[4] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 25, 2021) at Sec. 10 (j), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

impact assessments, scans at multiple deployment phases, code reviews, and penetration testing.

As policymakers and stakeholders advance the use of SBOM across diverse sectors and use cases, Ericsson has encouraged NTIA to develop SBOM requirements that build on our own work in software security assurance. In particular, we recommend that SBOM should be delivered in a controlled manner with limited distribution to only trusted third parties according to contractual agreements which should include confidentiality and integrity protection and mutual authentication during the transfer process. SBOMs should not be publicly disclosed, and SBOM requirements should be applied based upon the criticality rating of the software rather than in a "one size fits all" fashion. Ericsson has contributed this input and others to the June 2-3, 2021 NIST Workshop on Standards and Guidelines to Enhance Software Supply Chain Security as well as in written form to NTIA as part of its June 17, 2021 Request For Comments on Software Bill of Materials Elements and Considerations.

Second, we take a holistic approach to ensure that security is built into our systems from the start with layered due diligence and industry-aligned controls. We have developed an internal governance framework for security and privacy by design, providing guidance for security assurance across the product life cycle. 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, an international guideline on Information Security Management.

Third, in addition to our standards activities, we contribute to industry and government-industry initiatives to ensure supply chain and 5G security. These include our

service on the Executive Committee of the Communications Sector Coordinating Council (CSCC), best practice publications through the Council to Secure the Digital Economy (CSDE), leadership in NSTAC subcommittees and the aforementioned work on the ICT industry's response during COVID-19 as well as strategic planning for upholding the resilience of communications networks for the next decade, and our ongoing work in the FCC's CSRIC. Ericsson has been engaged across several working groups in the most recent iteration of CSRIC focused on 5G security and plans to participate fully in the upcoming CSRIC VIII. We are also participating in the groundbreaking work of the DHS ICT Supply Chain Risk Management Task Force, a formal, action-oriented collaboration between industry and government. I serve on the Threat Evaluation working group and I co-chaired a working group to develop methods for companies to provide formal assurances about their supply chain risk management, resulting in a Vendor Supply Chain Risk Management Template published in April. This will help make requirements such as the NIST security standards and other risk guidelines more useful in real-world acquisitions.

Fourth, with all of the above in mind, Ericsson heartily supports openness and the evolution to increasingly open network architectures. 3GPP has produced secure, open, and interoperable standards for each generation of cellular technology. 5G is the most secure generation of cellular networks that 3GPP has standardized to date, providing security end-to-end across the network through the RAN, core, transport and service-based architecture. Building on this work in 3GPP, industry is now working to develop technical specifications for Open RAN through the O-RAN Alliance and other technical collaborations.

While Open RAN is a nascent architecture, the benefits of Open RAN are evident in our own Cloud RAN portfolio, which focuses on hardware/software disaggregation, cloudification, open automation, and orchestration. Decoupling software and hardware allows RAN software to run on vendor-independent hardware, increasing vendor diversity. Increasing intelligence and automation allows operators to use tools to automate and simplify network operations on these decoupled, independent cloud platforms.

Ericsson is also a leader in the O-RAN Alliance. Ericsson co-chairs two working groups, made more contributions to O-RAN specifications in 2020 than any other company, and has the second-highest number of open source commitments and unique authors. Ericsson is currently supporting, or plans to support, eight of the ten RAN interfaces under discussion by the O-RAN Alliance. We urge the government to recognize the openness evident in the marketplace today, and to foreswear use of government mandates or preferences to drive the marketplace toward any particular technology. Instead of mandating or expressing a preference for a particular architecture, policymakers should continue to follow the longstanding guiding principle of technical neutrality and allow the industry to adopt the architecture of its choice based on the technology and business risks, without forcing the market to make investment decisions that could create significant deployment bottlenecks and other risks for U.S operators.

Ericsson believes that while Open RAN itself will not directly result in more secure networks, over time it can help provide benefits that advance security such as open interfaces, cloudification, intelligence, and automation to enable increased vendor diversity, deployment flexibility, higher performance, and greater resiliency in the 5G RAN. In this nascent stage of

development, however, this new architecture may, in fact, create new security risks. Accordingly, Ericsson is providing leadership in the O-RAN Alliance's Security Focus Group, which has adopted official work items to address new security risks unique to O-RAN, and we have recently been appointed as its liaison to the GSMA Fraud and Security Group.

Regarding policy to facilitate Open RAN's development and deployment, Ericsson itself sees no barrier to deploying Open RAN solutions. Ericsson's Cloud RAN is a major step on the journey to a secure Open RAN solution that meets the needs of U.S. critical infrastructure. It allows operators to run Ericsson RAN software using non-Ericsson open hardware and the third-party cloud stack (e.g., platforms provided by IBM/Red Hat, Linux, HPE, Intel, and many others). Ericsson has every reason to ensure that the regulatory environment is not unfavorable to our own Open RAN products. We can find nothing that would impede Ericsson or any other vendor from competing in the marketplace for Open RAN products and services.

Finally, what can the Committee do to support all this? First: Pass, implement, and oversee legislation to promote wireless security. We commend Committee Members for developing and engaging with industry on the proposed legislation that is the subject of this hearing, and we look forward to working with you on these bills as you consider them.

Second: Support actions to accelerate 5G deployment. Accelerated 5G deployment will advance the security of the 5G supply chain. Again, wireless and 5G infrastructure should qualify for funding in any broadband infrastructure funding legislation. The U.S. has the most innovative and competitive high-tech marketplace in the world, and a major key to that success is the fact that the market determines which technologies win, and which lose. Governments tipping the scales in the technology arena generally do not generate desired outcomes, and it

would be a mistake to push innovators onto any particular technological path—especially in an area in which technical specifications are still being developed. Ericsson thus asks that the Committee support technological neutrality, rather than requirements or preferences designed to push the market toward any particular type of network deployments.

Third: Continue to enable a secure and robust marketplace of trusted suppliers. Because global and domestic security are intertwined, it is imperative to ensure the long-term viability of a competitive, diverse global market of trusted and secure suppliers. The Committee should recognize and promote the value of leveraging strategic co-dependencies among the U.S. and its partners and allies, and develop policies that foster a diverse, trusted, global market of suppliers that deliver high performing, secure, and energy efficient network products to U.S. operators.

Fourth: Keep holding hearings on the subject of 5G security. Hearings like this highlight what industry and government agencies are doing to ensure a secure 5G world and maintain pressure on us to stay true to our security commitments.

* * *

On behalf of Ericsson, I thank the Committee for its leadership in this area. We look forward to continuing to work with you, and I look forward to your questions.