5G Supply Chain Security: Threats and Solutions

Testimony of Steven K. Berry

President and CEO

Competitive Carriers Association

Before the

United States Senate

Committee on Commerce, Science, and Transportation

March 4, 2020

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to testify about the security and integrity of the telecommunications supply chain, both for existing wireless networks and for our nation's 5G future.

I am testifying on behalf of Competitive Carriers Association ("CCA"), the nation's leading association for competitive wireless providers. CCA is composed of nearly 100 carrier members ranging from small, rural providers serving fewer than 5,000 customers to regional and nationwide providers serving millions of customers, as well as vendors and suppliers that provide products and services throughout the mobile communications ecosystem.

CCA and its members fully support efforts to protect and harden networks from cybersecurity and other national security threats. Press reports and actions by the federal government continue to underscore the threats posed by certain companies and foreign adversaries. To address these threats, I particularly commend this Committee's bipartisan leadership in sending the Secure and Trusted Communications Networks Act to the President for enactment. This important legislation addresses several key concerns of competitive carriers that are working to secure their networks. In particular, the legislation provides certainty regarding what actions small carriers must take to modify their existing networks and establishes a fund to ensure that resources are available.

Beyond the immediate attention on network security, we must also not lose focus on the economic security threats we face as a nation as we compete globally to provide the latest innovations, powered by wireless communications. Establishing American leadership for 5G network deployments, including the potential for a greater role in the 5G supply chain, is an important goal, and one that can only be achieved by ensuring that all Americans have access to the latest services, both in urban population centers as well as rural America. In fact, rural areas stand to enjoy the most immediate and significant benefits through expanded access to the latest wireless services. No one will win the so-called "race to 5G" without connecting the millions of people living in rural America.

While wireless networks are providing connectivity for innovations ranging from health and public safety advances to economic and social transformations, these connections must be secure. All carriers are therefore focused on ensuring that they are providing secure connectivity amidst an ever-growing array of potential threats. The transition to 5G networks provides an opportunity for all carriers to build in security as a basic function of network architecture and management.

Security threats are particularly acute for carriers that have equipment or services in their networks from companies deemed by federal agencies, including the Federal Communications Commission ("FCC"), to pose a "national security threat to the integrity of communications networks or the communications supply chain." To be clear, most CCA members do not have covered equipment in their networks. Those that do often provide service to their own rural communities, operating where no other carrier will provide service and at the thinnest of margins to connect their neighbors. These companies are owned by and employ Americans in their local communities, and I can assure you that these patriots want to take whatever steps are necessary to ensure our national security.

Whether or not a carrier has covered equipment in its immediate network, removing insecure network elements is a priority shared across the industry. Telecommunications networks provide value to all consumers through the network effects of connectivity, and networks must interconnect with each other. Further, through roaming and other arrangements between carriers, as you travel the country you have likely enjoyed service from rural carriers, whether you realize it or not. Accordingly, all networks must be secure.

This hearing is timely, with actions being taken not only by Congress, but also by the FCC and an Executive Order from the President. While the challenge is significant, and the legislative and regulatory policy directions are unprecedented, I have confidence that appropriate policies from the federal government will provide all carriers with the guidance and certainty they need to secure telecommunications networks. Through cooperative efforts and flexible policies, and funds for replacement, the removal of covered networks elements, where necessary, can be achieved. Such action will support new technologies and innovations while allowing market forces to advance secure services and make the latest wireless technology available for all carriers, whether they serve customer bases that are rural, regional, or nationwide.

All Carriers Must have Clear Guidance from the Federal Government Regarding Security

As a foundational step, all carriers must have the information and guidance from the federal government to confidently make decisions to secure their networks. With respect to the need for clarity, I appreciate the clear message sent by Congress through the Secure and Trusted Communications Networks Act regarding what network equipment is deemed to be insecure and must be removed from existing networks. This clarity is particularly important for smaller carriers that may not have dedicated staff focused exclusively on security issues or may not have the necessary clearances to engage directly with the intelligence community regarding potential threats.

I strongly encourage the federal government to continue to provide clear, unambiguous directions regarding the national security needs for communications networks so that government and industry can define a clear pathway for enhanced security and allocate resources to sustain these priorities. Such efforts help improve the security hygiene across the entire telecommunications industry, for small carriers and nationwide providers alike. Provisions in the Secure and Trusted Communications Networks Act that facilitate information sharing, specifically for smaller providers, will help advance this goal.

CCA has taken several steps to ensure that our members have access to the information they need to make confident decisions regarding potentially sensitive issues. For example, nearly a year ago approximately three dozen CCA members, including members with and without covered equipment, participated in a bipartisan, classified briefing on wireless security issues with the U.S. Senate Select Committee on Intelligence. I would like to thank Senators Warner and Rubio for hosting CCA members and key leaders from the Intelligence community to ensure that all carriers are provided with the information they need to make decisions to provide secure telecommunications services to their customers.

I am also very pleased that we were able to continue our educational effort by partnering last year with the U.S. Chamber of Commerce to conduct three Rural Engagement Initiative sessions. At these events we brought together numerous stakeholders, including representatives from Tier II and Tier III carriers serving rural areas, security experts from leading American and international vendors and suppliers, and key senior government officials from the Department of Homeland Security, Department of Justice, Federal Communications Commission, and Department of Commerce together in three different locations – Denver, CO, Jackson, MS, and Chicago, IL – to have frank discussions regarding current threats, potential solutions, and the roadmap for network operations in the years ahead. These conversations allowed both government and industry to gain a better sense of the strategic threats, and a clearer understanding that there is no one-size-fits-all solution to mitigating these threats. I truly appreciate our partnership with the U.S. Chamber of Commerce on this effort to bring critical information to all carriers. I also would like to particularly thank the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") for taking a lead role on behalf of the United States Government in these sessions, which brought tremendous value to competitive carriers and facilitated the direct flow of information between government and industry stakeholders. Building upon these conversations, I look forward to welcoming CISA as a keynote speaker at CCA's upcoming Mobile Carriers Show later this month.

Congress has Provided Clear Authority and Established a Fund to Secure Existing Networks

The Secure and Trusted Communications Networks Act not only provides clarity regarding what elements must be removed from existing networks, it importantly creates a fund to facilitate replacement for smaller carriers serving rural areas. I completely agree with your remarks, Chairman Wicker, on the Senate floor late last year that "some things are worth paying for, and protecting America, protecting our electronic system, our broadband communications … is worth paying for."

I am encouraged that this sentiment shares bipartisan support not only in Congress but also at the FCC. As FCC Commissioner Geoffrey Starks noted last fall at CCA's Annual Convention, "This is a national problem that deserves a national solution, and we shouldn't expect small carriers – who acted legally and in good faith – to replace their insecure equipment on their own." Recent Congressional action will provide needed resources for the replacement of covered equipment, an important step that is particularly needed for carriers who are unable to cover the costs of replacement without financial assistance from the federal government.

As the new fund is established and administered by the FCC, I am hopeful that resources will be available so that carriers can move expeditiously to replace covered network elements. This means that after a carrier with covered equipment has established a clear plan for replacement and removal of networks elements, they will have access to funding both as the process begins as well as at specified benchmarks throughout the process. Such access to needed resources recognizes that networks that were not initially economical to construct absent support mechanisms are unlikely to be able to finance the project management process without resources available long before certification that covered elements have been completely removed. Additionally, as the removal process moves forward, policymakers should allow for carriers to triage their networks and focus on the most significant vulnerabilities first. Specifically, policymakers should consider prioritizing replacement of core network and routing elements first, and radio and edge network elements thereafter, in recognition of using available resources to prioritize the highest potential threats.

While the legislation that recently passed establishes a swift one-year timeframe, I appreciate the inclusion of a waiver process to ensure that carriers that are unable to complete changes to their networks in such a rapid fashion remain eligible for support. Several factors, including available spectrum resources, equipment availability, limited windows to build in certain harsh geographic areas, permitting processes, the need for testing and configuration of new equipment, and even the availability of a properly trained workforce will all impact the time necessary for each impacted carrier to complete the transition process.

Going forward, I would be remiss not to mention concerns from our carrier members that reverse auction procedures used to distribute support for providing service in rural areas can lead to a race-to-the-bottom where low costs are prioritized above all else. Several carriers that have covered equipment in their networks today made vendor selections a decade ago in order to meet the reverse auction structure of Mobility Fund Phase I, where winning auction bids were those that had the lowest cost to serve the greatest number of road-miles. Despite there being no prohibited vendor selections at the time, it is now clear that this mechanism led to undesirable consequences for several carriers. While the FCC now has rules in place prohibiting using USF support for specific vendors going forward, security priorities should be appropriately funded so that other unintended consequences of funding least-cost networks can be avoided in the future. All funding recipients must be good stewards of taxpayer funds, but we should not simply fund the cheapest possible networks at the expense of all other priorities.

There should be some mechanism in the funding process that recognizes and rewards resiliency and security enhancements, prioritizing providing reliable and secure connectivity for consumers.

Replacing Covered Network Elements Must Precede Decommissioning to Maintain Connectivity

With clear guidance regarding network elements that pose security threats and a newly established fund available to replace them, carriers are eager to begin the work to transition their networks and continue to move forward to best serve their customers. To ensure that Americans in rural areas do not lose connectivity during this process, including to voice connectivity and 9-1-1 emergency services, important safeguards must be in place.

While those inside the beltway often refer to the process as "rip and replace," in practice carriers will typically need to "replace, then rip" to ensure that the consumers served by rural carriers do not lose service. This is a significant challenge for carriers, as a separate, standalone network must be established and stood up alongside current services before carriers can transition traffic to the new equipment and then decommission the covered elements. Networks in operation today have been built over years or even decades, and such a significant rebuilding will be all encompassing, including not only funding but also technical and logistical resources. Further, each carrier's network is unique, and accordingly there is not one plan or solution that can be followed by all carriers in this situation. Individual carriers' plans may be particularly challenging based on any given carriers' spectrum portfolio, which will need to support both new and legacy networks during the transition process, as well as the carrier's access to backhaul and other network characteristics. Again, only a few CCA carrier members have covered equipment in their networks, but all carriers understand the collective impact on their colleagues, and recognize that successfully addressing this challenge now will help everyone as we move to 5G.

Additionally, some covered equipment is outdated technology that is no longer manufactured or supported for new construction by any vendor. Equipment manufacturers generally are no longer making 2G and 3G equipment, and it would make little sense for any carrier to deploy a 2G or 3G network today. Accordingly, while the Secure and Trusted Communications Networks Fund should not create a windfall, resources should be available for carriers to provide like-for-like services that leave carriers more prepared at the end of the transition process to utilize other resources to upgrade networks to the latest generation of services in the future. For example, if a network with covered elements supports 2G and 3G CDMA voice products, the replacement should also support voice services, even if this means an enhancement in the network to support VoLTE voice services that could subsequently be upgraded as the carrier deploys 5G. This approach will ensure that the transition process does not leave a rural area stranded on legacy technologies while the rest of the industry advances. That is not a windfall but a reality reflecting the state of today's technology.

New Technologies can Help Secure Networks; Mandates should not Stifle Innovation

Removing covered network elements, as supported by the Secure and Trusted Communications Networks Act, is a critical step to secure today's networks, and several concepts included in the Act will also help secure the 5G networks of the future. For example, the Act requires the FCC to "develop of 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." Applied in a neutral fashion, this list can provide guidance to all carriers regarding secure equipment options for current and future network deployments, including end-to-end equipment used by most carriers today as well as increasingly virtualized and open source equipment and services.

As 5G wireless services provide increased potential to transfer network services from physical equipment to software, new technologies are increasingly coming to the market, including Open Radio Access Network ("ORAN") equipment. ORAN presents exciting new opportunities, with the potential to disaggregate functionality to increase efficiency and reduce costs. I encourage further research and development to explore virtualized solutions. ORAN may provide opportunities to increase security by breaking down the network stack and allowing multiple vendors to provide off-the-shelf components and services that when working together appropriately provide unified services. The potential for introducing American vendors into the ecosystem has tremendous benefits, but each layer must be sufficiently vetted for security. Particularly in greenfield network builds, ORAN can provide opportunities for new network designs that do not need to be integrated to legacy networks. For example, DISH, a CCA member, has announced plans to start deploying its standalone ORAN 5G network this year in the United States.

However, policymakers should not mandate which technologies are used in wireless networks, but instead should encourage research into new, secure technologies to enhance customer choice, innovation, and cost savings. For carriers with existing network infrastructure, additional research may facilitate increased ORAN deployment as well, and it is important that all network operators are positioned to manage additional steps for interoperability across multiple vendors. Absent a secure deployment approach, the increased number of access points that can present opportunities for additional vendors can expose additional entry points for bad actors. While ORAN equipment may be designed for network efficiencies, these technologies are not necessarily designed with the specific goal of enhancing security.

If new technologies like ORAN are successful, they will compete successfully in the marketplace. We must be mindful, however, that mandating using specific technology could require additional time for carriers seeking to replace covered elements from their networks, presenting a question of competing goals for policymakers. Smaller providers often rely on one or a small number of equipment providers for end-to-end services and do not have regular access to expansive test beds to vet all network elements. Carriers will continue to rely on existing trusted vendors, and may not be prepared for interoperability and system integration costs involved with multiple providers. They can ill afford to discover errors after deployment and operations are turned up to provide service and may have additional burdens to determine the cause of an error if there is a service outage. Further, smaller carriers depend on shared economies of scale for equipment with their larger competitors and are not in a position to drive the ecosystem. As previous technologies have been deployed at scale, smaller carriers can obtain economical access after deployment by larger carriers. Some smaller competitive carriers have also expressed concerns that an exclusive focus on new technologies that are not yet fully standardized or vetted could risk cannibalizing existing, trusted equipment providers.

As we seek to advance technologies and innovate, policymakers must ensure that the United States telecommunications industry does not lose access to trusted suppliers in the pursuit of potential new and exciting technologies of the future.

Additionally, I applaud inclusion in the legislation the creation of an information sharing program, led by the National Telecommunications and Information Administration and in cooperation with several other leading agencies, to share information regarding supply chain security risks with trusted communications providers and suppliers. This program can help ensure that all stakeholders have the information they need to continue to make decisions to secure networks into the future.

* * * * *

In closing, I would like to again congratulate this Committee for its leadership in passing the Secure and Trusted Communications Networks Act. As it is implemented, CCA is committed to working with Congress, the Administration, and all stakeholders to accomplish the unprecedented task of removing certain equipment out of telecommunications networks and ensuring network operations proceed using trusted vendors, all while maintaining communications services for millions of Americans in rural areas. Building upon these efforts to secure existing networks, we also have an opportunity to ensure that security is a pillar of 5G networks as they expand throughout our nation.

Thank you for the opportunity to testify at this important hearing, and I welcome any questions.