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

In the Matter of Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 to the Commission's Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain	)	WC Docket No. 18-89

COMMENTS OF COMSOVEREIGN CORPORATION

Dustin H. McIntire, PhD
Chief Technology Officer
COMSovereign Holding Corp.

May 20, 2020

TABLE OF CONTENTS

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

In the Matter of Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 to the Commission's Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain	)	WC Docket No. 18-89

COMMENTS OF COMSOVEREIGN CORPORATION

COMSovereign Holding Corp. ("COMSovereign")[1] respectfully submits the following comments on the *Public Notice* issued by the Federal Communications Commission ("FCC" or "Commission") in the above-captioned proceeding.[2]

I. INTRODUCTION AND SUMMARY

COMSovereign enthusiastically supports the Commission's efforts to implement Section 4 of the Secure and Trusted Communications Networks Act of 2019 ("Secure Networks Act")[3], which gives rural and small communications providers the financial resources needed to guarantee the security of their communications networks for the future. Given the reality of the

---

[1] COMSovereign is a publicly traded, U.S.-based, small business with a wide portfolio of 5G-related telecommunications and technology companies, including Dragonwave-X, Drone Aviation Corporation, InduraPower, Lextrum, Silver Bullet Technology, and VEO. This diverse array of organizations provides products and services for both telecommunications companies and federal and state agencies alike.

[2] *Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 to the Commission's Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, Public Notice, DA 20-406, WC Docket No. 18-89 (rel. Apr. 13, 2020) ("*Public Notice*").

[3] Secure and Trusted Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158, § 4 (2020) (Secure Networks Act).

contemporary global economy, the international use of outsourced labor, and a reliance on complex and integrated information and communication technology services ("ICTS") supply chains, it is crucial that American vendors diligently audit goods and services moving through their network supply lines. The 5G evolution will usher in a novel technology paradigm where services, applications, and network infrastructure are interconnected. Therefore, COMSovereign believes that a "cradle to grave" approach to a product's lifecycle is critical to guaranteeing national security in the ICTS supply chain. COMSovereign already manages the product design, maintenance, and disposal stages in its own business. The Commission should implement similar product oversight in the ICTS supply chain by integrating Section 4 of the Secure Networks Act into its current proceeding.[4]

A key component of the effort to secure America's telecommunications networks will be the Commission's creation of a well-vetted list of suggested replacement communications equipment and services.[5] Prior to issuance of such a list, the Commission should clearly define a set of qualification criteria for both vendors and specific equipment to be added to the list, and establish a method for demonstrating compliance with those criteria. Standards bodies can be valuable sources of input for setting benchmarks for supply chain security, and the Commission should rely on these standards for determining inclusion on the replacement list. Moreover, the Commission's suggested replacement list for communications equipment should include virtual

---

[4] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11433, para. 26 (2019) ("*Report and Order, FNPRM, and Information Collection Order*").

[5] Section 4(d)(1) of the Secure Networks Act directs the Commission to "develop a list of suggested replacements of both physical and virtual communications equipment, applications and management software, and services or categories of replacements of both physical and virtual communications equipment, applications and management software, and services."

equipment and services, and the list should be updated as frequently as feasible—at a minimum, quarterly. Once the list is established, the Commission should make it publicly available. Finally, the Commission should adopt a flexible approach to reimbursement budgeting and equipment replacement deadlines to ensure efficient replacement processes and appropriate allocation of taxpayer funding under the proposed reimbursement program.

II. COMSOVEREIGN IS AT THE FOREFRONT OF SECURE COMMUNICATIONS TECHNOLOGIES.

COMSovereign holds a portfolio of communications technology companies whose combined capabilities enable connectivity across the entire data transmission spectrum. COMSovereign is a leading U.S. pure-play communications provider capable of deploying 4G, LTE Advanced, and 5G-NR telecommunications systems. COMSovereign also has a number of virtual network companies in its portfolio. Most recently, COMSovereign announced its intent to acquire Virtual Network Communications, Inc., further expanding its array of advanced network companies.[6] Virtual Network Communications, Inc. is a developer of fixed and mobile broadband solutions for wireless networks operated by commercial and government defense customers alike.

COMSovereign prioritizes the security of its technologies. COMSovereign and its portfolio companies develop much of their hardware and software in their own North American facilities. Moreover, COMSovereign uses well-established partners and suppliers that do business directly with the Department of Defense. Aside from being a trusted federal government partner, the company also supplies some of the largest telecommunications and

---

[6] Press Release, COMSovereign, COMSovereign Holding Corp. Announces Letter of Intent to Acquire Virtual Network Communications, Inc. (Feb. 27, 2020), https://coms.irpass.com/COMSovereign-Holding-Corp-Announces-Letter-of-Intent-to-Acquire-Virtual-Network-Communications-Inc.

technology companies in the U.S. To ensure the integrity of its ICTS supply chain, COMSovereign inspects all source code that it receives from vendors and compiles it using internal, trusted tool chains.

III. THE FCC'S LIST OF SUGGESTED REPLACEMENT EQUIPMENT AND SERVICES MUST GUARANTEE THE INTEGRITY OF THE ICTS SUPPLY CHAIN.

As directed by Congress, the Commission should promote the security of U.S. ICTS supply chains by developing a list of suggested communications replacement equipment and services based on particularized ownership and supply chain information provided by potential suppliers.[7] This list should be vendor specific as well as product-specific, and should include suppliers of virtual network equipment and services. The Commission should establish set criteria to determine inclusion on the replacement list, drawing on recommendations from standards bodies. The Commission should also explain how vendors can demonstrate compliance with the criteria. The Commission should update the list as frequently as feasible and make the list publicly available. Establishment of a well-vetted and verified list of replacement equipment and services will further the government's goal of securing the ICTS supply chains.

Criteria. Before generating a list of acceptable replacement equipment and services, the Commission should clearly define criteria for inclusion for both vendors and equipment. Once there are criteria for both vendor and equipment inclusion on the replacement list, the Commission should detail how such entities can demonstrate compliance with the criteria.

[7] Section 4(d)(1) of the Secure Networks Act obligates the FCC to "develop a list of suggested replacements of both physical and virtual" communications equipment for the "rip and replace" process.

As an initial matter, the replacement list should reflect the objectives of the Secure Networks Act by promoting vendors that manufacture and supply equipment from the U.S. and U.S.-allied countries.[8] Commissioner Starks highlighted this important objective in the *Report and Order*: "[W]e must seize this opportunity to encourage the growth of American technology for next generation networks. American 5G equipment will be safer because we can be confident about it observing best practices and protecting our intellectual property and privacy from foreign actors."[9] In addition, the list should include vendors who have demonstrated capability of ensuring a sterile chain of custody for network components and services, from product design through disposal. The Commission's list should also include equipment and service vendors that rigorously audit the security of their own ICTS supply chains, such as COMSovereign.

Standards bodies have an important role to play in developing standards that promote network security, and compliance with such standards can be used as a benchmark for determining vendor and equipment supply chain security. As an active member of the Telecommunications Industry Association ("TIA"), COMSovereign participates in establishing open industry standards for defining supply chain security as well as quality metrics to be used for qualification. COMSovereign recommends that the Commission work in collaboration with existing standards bodies to assure the resulting standards will meet or exceed any thresholds for

---

[8] The purpose of the Secure Networks Act is to "prohibit certain Federal subsidies from being used to purchase communications equipment or services posing national security risks" and to "provide for the establishment of a reimbursement program for the replacement of communications equipment or services posing such risks." Secure Networks Act.

[9] *See Report & Order*, FCC 19-121 (Statement of Commissioner Starks). "[W]e need to begin researching how we can build networks that can withstand connection to equipment vulnerabilities around the world. One way to do this is to virtualize and diversify key parts of our networks." *Id.* (Statement of Commissioner Rosenworcel).

inclusion on the replacement list. The collaboratively developed open standards may also then be used for determining vendor and equipment supply chain security.

Inclusion of Product-Specific Information. The Commission's product and service replacement list should not only identify trusted vendors, but it should also specify the approved equipment and product components offered by each supplier on the list. This will avoid "white labeling" issues, where a component manufacturer removes their branding from a product or component and uses the branding requested by the purchaser. In this scenario, an approved vendor could be offering a product that is labeled as being U.S.-based, but that consists of components manufactured in countries that pose a national security risk to the ICTS supply chain. The Commission should ensure that product components undergo a careful review before supplier products and services are added to the approved vendor list.

Updating. The FCC should update its approved replacement vendor and equipment list frequently to keep pace with new technologies and innovations. If possible, updates should occur quarterly, at minimum. This will help guarantee that the most advanced products and services are made available to small and rural providers participating in the "rip and replace" program. The Secure Networks Act is specifically focused on guaranteeing the security of small communications providers, as the reimbursement program's eligibility is limited to those carriers with two million or fewer subscribers.[10] Therefore, regular updates would encourage investments in cutting edge American technology while closing the digital divide in insular and rural communities by ensuring that such next-generation communications capabilities are made available to all consumers.[11]

---

[10] Secure Networks Act § 4(b)-(c).

[11] Comments of the Rural Wireless Association, WC Docket No. 18-89 (filed Feb. 3, 2020) ("Limiting reimbursement to technologies that are comparable to what is already installed would

Virtual Equipment and Services. It is imperative that the FCC's replacement list include vendors and products offering virtual equipment and services. These types of services will comprise a large constituent of modern communications networks in the near future. Voice communications are no longer the primary communications traffic applications. Rather, most traffic now consists of video streaming from the edge to the core of a network, and emerging Internet-of-Things devices require virtual network capabilities.[12] The Commission should recognize this global trend and adopt a forward-looking approach in developing a replacement list that incorporates virtual products and vendors of such services.

Publicly Available List. Once generated, the Commission's replacement list should be made publicly available. Having this information easily accessible will promote use of secure equipment and services therefore furthering the Commission and Congress's goal of protecting the integrity of U.S. ICTS networks. A publicly available list will also ensure that companies of all sizes and levels of sophistication can easily learn about products and services that do not pose a risk to the communications networks or supply chains.

IV. THE COMMISSION SHOULD TAKE A FLEXIBLE APPROACH TO BUDGETING AND REPLACEMENT DEADLINES UNDER THE REIMBURSEMENT PROGRAM.

COMSovereign encourages the FCC to design a "rip and replace" framework that incorporates flexibility to account for carrier challenges and acknowledges that estimating the cost of ripping and replacing large network components is likely to be an iterative process.

---

disserve rural citizens and forego a unique opportunity to jump-start the deployment of advanced broadband networks in rural areas that have long been deprived of any access to adequate broadband services.").

[12] *See, e.g.* Cisco, Cisco Annual Internet Report (2018-2023) White Paper (Mar. 9, 2020), https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (estimating that the number of devices connected to Internet protocol networks will be three times that of the world population by 2023).

Incorporating these principles will aid carriers in accomplishing the Commission's goals of securing the supply chain. Finally, it is critical that the Commission implement verified disposal requirements for network equipment posing a national security risk to ensure that it does not reenter U.S. supply chains.

A. The Commission Should Maintain Flexible Expectations with Respect to Timing and Budget Estimates for Equipment Replacement.

Replacing equipment and services in the timeframe required by the Secure Networks Act[13] will depend on a number of factors, some of which will be outside of a carrier's control. The Commission should therefore build flexibility into its deadlines for "rip and replace" and grant individual extensions as needed.

Replacing network equipment poses several challenges. For example, communications providers such as cable operators, satellite carriers, and wireless and wireline communications providers, must schedule planned outages ahead of time with the FCC.[14] Providers also must be careful to ensure that outages can occur without compromising network integrity. Once the outage is scheduled and the equipment replaced, providers must factor in time to "test and evaluate" new equipment before final installation.[15] Another challenge is that industry has not previously had experience in undertaking such widescale network equipment replacements, which make initial time and budget estimates hard to calculate. To account for these obstacles,

---

13 Section 4 of the Secure Networks Act requires program recipients to finish the "removal, replacement, and disposal of any covered communications equipment or services" within a year after reimbursement funds are distributed by the FCC. Secure Networks Act § 4(d)(6)(A)). Secure Networks Act § 4(d)(6)(A)).

14 47 C.F.R. §§ 4.3, 4.9.

15 Comments of JAB Wireless, Inc., WC Docket No. 18-89, at 14 (filed Feb. 3, 2020).

the Commission should build flexibility into its timelines and grant extensions to carriers as needed, drawing on its authority under the Secure Networks Act.[16]

The Commission should also carefully consider how to structure the disbursement process to account for carrier differences and challenges, and the unique nature of this effort. While the Commission's proposal would issue initial support payments based on cost estimates,[17] the FCC should consider alternative approaches as the program progresses. For example, the Commission could establish phases for "rip and replace" efforts and release funding when certain milestones are met. Such a phased approach could reduce misappropriation by tying funding to replacement progress. In addition, as the program progresses, the Commission will be able to better estimate and validate removal and replacement costs to avoid misuse of taxpayer funds.

B. The Commission Should Implement Verified Disposal Requirements for Covered Network Equipment.

ICTS supply chain security auditing activities should not end with product retirement. Indeed, several record commenters note that any reimbursement program must cover legacy equipment disposal costs.[18] This "cradle to grave" equipment management approach ensures that next generation communications technology is secure both at the design phase and at the

---

16 The Secure Networks Act gives the Commission statutory authority to grant a six-month extension to all carriers under the reimbursement program and provides the FCC additional discretion to grant supplemental six-month extensions to individual carriers as necessary. Secure Networks Act § 4(d)(6).

17 *FNPRM* ¶ 149.

18 Reply Comments of the Rural Wireless Association, Inc., WC Docket No. 18-89, at 14 (filed Mar. 3, 2020); Comments of NTCH, Inc., WC Docket No. 18-89, at 7-8 (filed Jan. 31, 2020); Comments of Puerto Rico Telephone Company, WC Docket No. 18-89, at 16 (filed Feb. 3, 2020).

disposal phase. It is critical that disposed network equipment posing a national security risk does not end up back in the ICTS supply chain.

While the Commission's *FNPRM* provides applicant certification requirements and detailed reimbursement application entries, the FCC should also establish verified disposal requirements for network equipment.[19] To ensure proper equipment disposal, the Commission should require carriers to utilize certified electronic recyclers and should mandate reporting and verification requirements that facilitate supply chain auditing throughout the "rip and replace" process. This process would not only encourage environmental efficiency, but it would require that carriers be directly accountable to the public for their disposal processes.

V. CONCLUSION

In light of the foregoing, the Commission should integrate Section 4 of the Secure Networks Act into its "rip and replace" proposals to safeguard the integrity of the U.S. communications networks and supply chains. In doing so, it should develop an equipment replacement list that is component-specific and regularly updated. COMSovereign also urges the FCC to embrace flexible reimbursement deadlines and carefully consider approaches to reimbursement to promote efficiency and reduce potential waste.

Respectfully submitted,

/s/

Dustin H. McIntire, PhD
Chief Technology Officer
COMSovereign Holding Corp.

May 20, 2020

[19] The Secure Networks Act requires that providers detail regular equipment removal status updates. Secure Networks Act § 4(d)(8).