cca rural. regional. nationwide.®

Communications Networks Safety and Security

Testimony of Tim Donovan

President & CEO

Competitive Carriers Association

Before the

United States Senate Committee on Commerce, Science, & Transportation

Subcommittee on Communications, Media, & Broadband

Wednesday, December 11, 2024

Chairman Luján, Ranking Member Thune, and Members of the Subcommittee, thank you for the opportunity to testify about the importance of providing safe and secure connectivity for all Americans.

Competitive Carriers Association (CCA) represents communications providers ranging from small, rural providers, serving fewer than 5,000 customers, to regional and nationwide providers serving millions, as well as vendors and suppliers throughout the communications ecosystem. Our members are often the only provider for hundreds or even thousands of square miles of their service areas, providing life-saving connectivity across large swaths of rural America – including in your home states of New Mexico and South Dakota – for their subscribers, as well as millions of Americans who roam onto their networks.

CCA and its members thank this Committee for its continued focus on security and expanding connectivity to all Americans. This hearing is timely as new details of compromised networks fill headlines daily. While work must continue to analyze and to secure networks related to the Salt Typhoon breach, it is important to look at the broader threat landscape and for Congress and the federal government to take steps to promote safe and secure networks. This includes fully funding the $3.08 billion shortfall needed to complete the Secure and Trusted Communications Networks Reimbursement Program (STCNRP or Reimbursement Program) – often referred to as Rip & Replace – at the Federal Communications Commission (FCC), promoting work between communications providers and federal partners with clear and unambiguous guidance, and beginning work now to take steps in the 119th Congress to preserve and expand connectivity with a focus on security.

I. CONGRESS MUST FULLY FUND THE "RIP & REPLACE" PROGRAM.

CCA thanks this Committee for passing the Secure and Trusted Communications Networks Act (STCNA), which, among other provisions, created the STCNRP. This important program is part of a yearslong effort to address concerns related to communications equipment and services deemed by federal agencies, including the FCC, to pose a "national security threat to the integrity of communications networks or the communications supply chain," including the following benchmark steps:

- **August 13, 2018:** 2019 NDAA Section 889 enacted, limiting use of federal funds for untrusted telecommunications equipment.
- **March 12, 2020**: The Secure and Trusted Communications Networks Act of 2019 is signed into law after passing Congress with broad bipartisan support.
- **December 27, 2020**: Congress appropriates $1.9 billion to the FCC for the Secure and Trusted Communications Networks Reimbursement Program in the FY2021 Consolidated Appropriations Act with a priority for companies with under 2 million subscribers.
- **October 29, 2021**: FCC opens the filing window for applicants seeking support from the Reimbursement Program.
- **February 4, 2022**: FCC notifies Congress that they have received 181 original applications from 96 applicants requesting $5.6 billion and that current appropriations would not be sufficient to fully fund all approved applications.
    - STCNA requires the FCC to approve or deny applications within 90 days of submission but allows the FCC to extend that deadline by up to 45 days if additional time is needed to review. Exercising that option, the FCC extended the review deadline to **June 15, 2022**.
- **June 1, 2022**: FCC Chairwoman Rosenworcel informs Congress the FCC determined the gross cost estimate demand for the program was reduced to $5.3 billion and anticipated further reduction, but that appropriated funds will remain less than the demand from applicants. She notes three contributing factors:
    - The expansion of entities eligible for participation in the Program by the FY2021 Consolidated Appropriations Act;
    - Preliminary cost estimates of the Program did not consider the full range of costs that were ultimately reimbursable under law;
    - Providers reported increased costs since the program was funded due to supply chain issues, inflation, and project completion requirements by law.
- **June 15, 2022**: FCC Chairwoman Rosenworcel updates Congress on the FCC's progress reviewing "materially deficient" applications and allowing applicants to cure their

submissions. She also announces that absent additional appropriations, the FCC will apply the prioritization scheme specified by Congress for allocation funding on a pro-rata basis.

- **July 15, 2022**: FCC Chairwoman Rosenworcel informs Congress that the FCC has completed its review of applications to the Reimbursement Program, and announces in a Public Notice the granted applications for reimbursement, the approved cost estimates, and the approved prorated allocations.
    - FCC Chairwoman Rosenworcel notes a shortfall of $3.08 billion to fully fund approved cost estimates.
    - Chairwoman Rosenworcel announces the Commission will prorate reimbursement funds equally to each eligible applicant that have 2 million customers or less. The pro-rata factor is approximately 39.5%.
- **July 17, 2023:** Applicants approved for funding support are required to have submitted at least one reimbursement claim, and are required to complete the permanent removal, replacement and disposal of Huawei/ZTE communications equipment and services from their networks within a year of initial distribution of reimbursement funds.

Since 2023, the FCC has continued to update Congress on the status of the program, yet it cannot be completed without sufficient funding. As Chairwoman Rosenworcel noted in her most recent update to Congress, "[t]he consequences of the continued lack of full funding for the Reimbursement Program are significant for our national security and rural communities."[1] To be clear, while the program should have been completed this past July under Congress's initial timeline from the STCNA, significant amounts of covered equipment and services remain in place today because of insufficient funding. The FCC has had to use authority provided by Congress to grant 139 extensions of time, including 118 "based in whole or in part on the

[1] Letter from Jessica Rosenworcel, Chair, Fed. Commc'ns Comm'n, to Hon. Steny H. Hoyer, Ranking Member, H. Comm. on Approps., Subcomm. on Fin. Servs. And Gen. Gov't (Nov. 26, 2024), https://docs.fcc.gov/public/attachments/DOC-407870A1.pdf.

funding shortfall." While necessary, these extensions mean that the process is prolonged with increasingly disruptive impacts on the participating carriers and customers they serve.

A. Without full funding, many of your states will lose coverage; including for 9-1-1 and emergency services.

The situation is dire: rural telecommunications providers, especially in Western states, are being forced to decide where to remove equipment but not replace it, eliminating service both to their own subscribers as well as the tens of millions of Americans who roam onto their networks for connectivity, including for 9-1-1 and emergency services. For example, though five Reimbursement Program participants collectively serve under 200,000 subscribers, they connected over 60 million Americans last year who roamed onto their networks because no other service was available. These decommissioning decisions are permanent choices that are detrimental to service availability and even the feasibility of entire businesses. These decisions are agonizing for our Rip & Replace members because they live in the communities they serve. They know that if their network cannot carry a 9-1-1 call, it could be their neighbor, or someone from their own families, who is unable to access lifesaving services. Eliminating service in an area does not only affect that carriers' customers, but anyone who would roam onto their network, as they are often the only wireless provider serving much of their market. Millions of Americans, particularly in rural areas and on Tribal Lands, could lose basic connectivity.

Without Congressional action, the lack of STCNRP funding is forcing rural carriers to go out of business. This is not hypothetical. Without more funding, in the coming months, you will see companies go out of business – disconnecting service and eliminating jobs in your home states. To further underscore the impacts across large swaths of the country, the following are examples of impacts from CCA members participating in the STCNRP:

- A Reimbursement Program participant will be forced to reduce its coverage area by over 67% (over 31,000 square miles) in Arizona and nearly 64% (over 26,000 square miles) in Nevada.
- That same carrier would have a nearly 90% reduction in service in Utah, and the impacted areas include key military and national security installations.

- A Reimbursement Program participant in New Mexico will lose 70.2% of its current coverage area (over 19,000 square miles) leaving customers unserved.
- A Reimbursement Program participant in Colorado will be forced to reduce its coverage area by 73.8% (13,766 square miles).
- A Reimbursement Program participant in Wyoming will be forced to reduce its coverage by over 80% (nearly 4,000 square miles).
- A Reimbursement Program participant in Montana will be forced to reduce its service by over 62% (over 1,500 square miles).
- A Reimbursement Program participant that serves the Navajo Nation will likely reduce coverage in that area by 20-40%.
- A Reimbursement Program participant covering 122,000 square miles in the Rocky Mountains is deciding what portions of its network to decommission because of the funding failure. Its coverage area will need to be reduced by over 70,000 square miles, eliminating the only coverage roamers have available. This coverage area includes 40 military installations, 32 of which are in areas that will not retain service without full funding, including a strategic missile base. Further, only 91 healthcare facilities out of 456 will remain covered, and only 415 schools or other educational facilities out of 1,897 will be able to retain coverage. Over half of this provider's approximately 40,000 subscribers will be affected, as well as the 13-14 million roamers that use the network each year.
- A Reimbursement Program participant in Western states that connects approximately 20 million annual roaming customers, in addition to its own customers, would see service degraded or lost.
- A Reimbursement Program participant serving a large rural area in the Upper Plains cannot transition to 5G because it does not have full funding to remove untrusted equipment. The network, and the communities it serves, will degrade over time and the area will go from served to unserved.

- A Reimbursement Program participant in the South faces financial obligations beyond its prorated funding and faces dire implications in the absence of full funding even if they do not rip and replace.

B. Without full funding, untrusted equipment remains in place, including in locations near military bases and other areas of strategic importance.

This funding shortfall not only threatens the success of the Reimbursement Program and connectivity in rural America, but it also seriously compromises national security. As stated above, untrusted equipment remains in service right now, including some near military bases, airports, and other areas of strategic importance. Further, because this equipment cannot be properly maintained or upgraded, every day that passes increases the risk of catastrophic network failures. Because it is illegal to procure new equipment *and services* from untrusted vendors, carriers with this equipment cannot properly patch and upgrade software to defend against emerging threats or even perform basic maintenance. They cannot work with the equipment manufacturers to identify problems or resolve issues. If Salt Typhoon can hack major operator networks, then there is a flashing red light for Rip & Replace networks that do not have those resources.

The national security risk also goes beyond the Reimbursement Program participants. Because of the fundamentally interconnected nature of networks, a threat to one network is a threat to all. This impacts not only network interconnections, peering, and traffic exchange between networks, but also consumer access. For example, a customer who roams onto a network with covered equipment or services, because no other connectivity is available, could have their device compromised. It has been over six years since Section 889 was enacted, and the status quo is critically unsustainable.

The inability of Reimbursement Program participants to complete their projects in our own backyards also undermines America’s strength and leadership internationally. The United States has led the world in raising concerns regarding use of insecure communications equipment and services and has strongly urged Allies and other nations to remove covered equipment currently in use and prohibit future deployments. We must complete this process at home to maintain connectivity in many rural areas while addressing a national security mandate and demonstrating global leadership.

C. There are no other options for Rip & Replace carriers. Congress must provide $3.08 billion.

While FCC extensions of time have been necessary, there is little else the agency can do to support the STCNRP without additional funding. Additional time alone cannot provide the resources for work to continue. Indeed, 72% of the status updates filed on October 7, 2024 indicated that the lack of full funding continues to be an obstacle to completing the permanent removal, replacement, and disposal of the covered communications equipment and services in recipients' networks.[2] Fifty percent of the participants reported that they cannot complete the work required because of the funding shortfall.

This is not a partisan issue. It impacts Americans in red and blue states alike. Funding has bipartisan support in Congress and at the FCC. In addition to Chairwoman Rosenworcel's calls for necessary funding, Commissioner Carr has strongly called for Congress to close the funding gap, including in testimony earlier this year noting that:

> As a government, we have taken the smart step of ordering the removal of this insecure and high-risk Equipment – gear that proliferated in rural networks near some of our military's most sensitive facilities – and we have said that we would compensate covered providers for the costs of removing and replacing that gear. We need to make good on that promise.[3]

D. Congress has an immediate opportunity to address this issue in the FY2025 NDAA.

I am encouraged by, and deeply appreciative of, recent legislative developments towards meeting this critical moment and providing the desperately needed funding. The Senate Amendment to H.R. 5009 – WILD Act [Servicemember Quality of Life Improvement and

[2] Letter from Jessica Rosenworcel, Chair, Fed. Commc'ns Comm'n, to Hon. Steny H. Hoyer, Ranking Member, H. Comm. on Approps., Subcomm. on Fin. Servs. And Gen. Gov't (Nov. 26, 2024), https://docs.fcc.gov/public/attachments/DOC-407870A1.pdf.

[3] *Budget Hearing – Fiscal Year 2025 Request for the Federal Communications Commission Before the H. Comm. on Approps. Subcomm. on Fin. Servs. And Gen. Gov't* (May 16, 2024) (testimony of Brendan Carr, Comm'ner, Fed. Commc'ns Comm'n).

National Defense Authorization Act for Fiscal Year 2025] (NDAA) includes provisions to increase the STCNRP authorization to the level needed to complete the program and allow the FCC to immediately access the funding necessary. I thank the Senators, Representatives, and staff – including members, leadership, and staff on this Committee – for their steadfast work to arrive at this point. CCA supports this effort and urges Congress to swiftly pass this important legislation and send it to the President for enactment.

II. FEDERAL POLICYMAKERS SHOULD TAKE STEPS TO SUPPORT INDUSTRY SECURITY EFFORTS.

Congress should support efforts to increase collaboration between federal agencies and carriers to bolster network security and to remove barriers and uncertainty. This includes updates to information sharing, clear and consistent security requirements, and a recognition of the unique challenges faced by smaller carriers, including limited resources.

All carriers must have clear and unambiguous guidance and information from the federal government on network security. Obtaining this information can be particularly challenging for smaller and rural carriers, with limited resources and staff, that are unlikely to have in-house personnel, let alone teams of professionals, with appropriate and often necessary security clearances sitting alongside federal partners on a day-to-day basis. Without better channels for information sharing, there can be times that, even when federal partners want to help, assistance is minimal because the lack of clearances prohibits sharing anything other than unclassified/public information. For example, in the ongoing efforts surrounding Salt Typhoon, without sharing of intelligence, many carriers have late or limited indicators of compromise to go hunting for or understanding of how hackers got in, hampering the ability to respond and further secure their networks.

While lists of trusted or untrusted vendors for equipment and services are helpful, efforts must go further. These lists have primarily focused on network equipment and vendors, yet carriers may not have visibility deeper into supply chains to avoid chipsets, modules, or other devices that could create vulnerabilities. Information sharing efforts targeting small and rural carriers like the Communications Supply Chain Risk Information Partnership (C-SCRIP) at the National Telecommunications and Information Administration (NTIA) are helpful and should be expanded, including with appropriate resources to assist all carriers. Most small and rural carriers do not have the resources to participate in ongoing public/private initiatives on security such as the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) Communications Sector Coordinating Council. Our carriers truly need federal partners in the fight with us, and they need access to the information and resources required for staying ahead of the seemingly never-ending game of security whack-a-mole.

Information sharing should facilitate collaboration not only between federal partners and carriers, but also among carriers. This can create difficulties because our members report that they do not know which other carriers have had cybersecurity issues in part because, as one said:

> We aren't allowed to talk to others, even if we know something, we probably can't share it. This hinders communications and makes things really complicated. We don't know who we can talk to, or what we can talk about with carriers. Somehow, we all need to be brought up to the same level, all brought under the same tent, and be allowed to have open and honest discussions with the other carriers. We need to learn from each other. Right now, we can't do that. By doing things the way the government has, in some ways they have made things worse.

In addition to real-time information sharing, policymakers must take steps to ensure security requirements are clear and consistent across the federal government. Today, there are many different standards and requirements that carriers must consider, with new layers constantly being added. These range from industry standards, for example, those from 3GPP and other international standards organizations, as well as various requirements or recommendations from the FCC, CISA, and the Department of Commerce's National Institute of Standards and Technology (NIST). Even if well-intended, the lack of coordination is a significant challenge to the implementation of successful cybersecurity plans. There can be major differences between requirements from CISA and what is required by an agency as part of specific programs administered by the FCC, NTIA, or the Treasury or Agriculture Departments. At least in terms of the federal government, minimizing the agencies involved and synchronizing security-related requirements would foster clarity and consistency and also reduce the associated regulatory burdens so providers with limited resources can use those resource to actually improve their network security.

As breaches occur, it is important to balance alerting consumers and national security authorities with understanding and resolving threats, especially for carriers with limited staff and resources. Our members report significant problems with overly burdensome data breach reporting requirements. For example, the FCC's *Data Breach Order* undermines Congress's connectivity goals by unnecessarily and unlawfully imposing significant compliance costs on smaller carriers, most of which are small businesses that lack dedicated privacy teams and in-house attorneys to navigate the requirements that the FCC has stacked atop existing state and federal data breach notification laws. In addition, the FCC proposed requiring broadband providers to develop and implement detailed risk management plans for Border Gateway Protocol (BGP) security. These requirements should account for the cumulative regulatory burdens on carriers. The same team or individual may be struggle with these requirements as well as other cybersecurity proposals related to Wireless Emergency Alerts (WEA), the 5G Fund, and CISA's upcoming Cyber Incident Reporting for Critical Infrastructures Act (CIRCIA) reporting framework because of lack of human and financial resources to keep up.

It would be helpful to have one set of centralized authority and directive on cyber hygiene. For example, CCA encouraged the FCC to coordinate with CISA and industry-driven efforts instead of independently regulating. CCA also encouraged CISA to synchronize its CIRCIA reporting with the FCC's reporting requirements as encouraged by Congress. Congress should ensure needed flexibility with government standards with capacity building for carriers, especially smaller ones. Using existing programs can also reduce costs and encourage broader participation.

Federal policymakers should also be aware of specific challenges faced by smaller carriers. Beyond having smaller teams with a potential lack of security clearances, many smaller carriers rely on their vendor partners for aspects of security hygiene, monitoring, and response. Smaller carriers do not have the buying power or scale to demand specific security procedures. They rely on broader economies of scale and industry investment to support these efforts instead of costly bespoke equipment and services.

Finally, federal policymakers should continue to encourage and invest in new solutions, including research, development, and growth of Open RAN technologies and continued support for trusted vendors. This investment will not only support network security domestically but will also have international impacts that advance American leadership. Today, a large portion of the world's communications networks rely on equipment from untrusted vendors, raising significant security concerns. CCA believes that continued growth of Open RAN can provide an important alternative by enabling a multi-vendor ecosystem that decreases the dependence on untrusted vendors while promoting competition and innovation. However, policymakers should not mandate technologies – if new technologies deliver on their promise, they will compete and succeed in the marketplace. CCA also supports continued partnerships like that between CCA member Cape and the U.S. Government to support strategic communications services to address concerns around security vulnerabilities.

III. IMPORTANT CONSIDERATIONS FOR THE 119TH CONGRESS.

There are several key policy issues Congress should prepare for consideration in the upcoming 119th Congress that are necessary to preserve and expand connectivity, each with aspects impacted by security issues.

A. Universal Service Fund (USF) Reform and Litigation.

I commend you; your staffs; those of Sens. Klobuchar, Peters, Moran, and Capito; and their House Energy & Commerce Committee counterparts for your diligent efforts to create a bipartisan working group for reforming the USF. All CCA members have an interest in ensuring that all Americans have access to the latest broadband services, especially those in rural and high-cost areas. CCA appreciates Congress's support for bipartisan policies that foster sufficient and predictable USF support and that advance the universal service goals of Section 254 of the Communications Act, as amended.

The job of universal service is not complete – there are still areas where coverage will continue to need to be filled in and deployed to meet the overall objectives of ubiquitous voice and broadband services. Even where deployments have occurred, ongoing support for operating expenses – including maintaining an appropriate security posture – demand support from USF to continue to provide service. Most rural carriers operate on extraordinarily thin margins, so threats to USF hurt their ability to upgrade their cybersecurity infrastructure. Failure to update and direct USF programs to preserve and to expand ubiquitous connectivity will lead to continued consolidation of smaller carriers and carriers serving rural America, reducing coverage in areas uneconomical to serve absent support.

Especially considering the subject of today's hearing, Congress should ensure that resources are available to promote secure networks, especially for smaller carriers serving rural areas. USF reform could be an opportunity to promote cybersecurity best practices. In addition to considering USF eligibility for more carriers and areas, funding for cybersecurity compliance could be part of an operational expenditure fund or part of an existing fund.

Further, recognizing the importance of security, the FCC should consider alternatives to awarding USF support through reverse auctions. These create a race-to-the-bottom where cuts to security may be necessary to access support. Indeed, a previous reverse auction for the Mobility Fund Phase I drove the deployment of significant amounts of equipment now subject to the STCNRP, because those vendors made their equipment and services available at the lowest cost.

The USF is also under threat in the courts. The Supreme Court granted certiorari in a case that could destroy the USF. The litigation questions the fundamental delegation of authority for the USF from Congress to the FCC, and from the FCC to the Universal Service Administrative Company (USAC). The FCC and CCA, among others, are fighting to protect the USF from these attacks. We appreciate the leadership from several Members of Congress, including on this Committee, in previously supporting USF in court against litigation threats by submitting an amicus brief, on bicameral, bipartisan basis, supporting the FCC's defense of the USF in the Fifth Circuit. If the USF is undermined by this litigation, it could have disastrous impacts on broadband deployment in the United States. Although CCA maintains that Section 254 provides more than enough authority for the FCC to administer the USF, Congress could provide additional clarity to protect the USF from future, spurious litigation attempts and should be prepared to act quickly if a court decision undermines the USF.

B. Permitting Reform.

The ability to site, build, and upgrade network equipment is also important for reinforcing network security. CCA members often face unique environmental and geographic challenges that complicate infrastructure work, and increased costs associated with permitting can take up resources that could otherwise be dedicated to enhancing security. Siting reform is critical to overcome major potential barriers to broadband deployment. In the next Congress, CCA encourages common-sense historic and environmental preservation reforms, improved siting standards, and greater CCA member access to Federal lands. CCA also strongly believes that meaningful broadband infrastructure reform need not pit carriers against federal agencies, states and municipalities. Congress should consider programs and legislation that incentivize state and local governments to facilitate deployment, including through appropriately staffing review offices.

C. Spectrum Auction Reauthorization.

Access to additional spectrum allows carriers to continue to improve coverage, capacity, and upgrade to the latest – and often most secure – equipment and technologies. I echo calls from many on this Committee to reinstate the FCC's general spectrum auction authority. Congress should also facilitate, improve, and maximize public/private collaboration and interagency cooperation in federal spectrum management and continue to support providing carriers of all sizes with meaningful opportunities to bid on and win spectrum at auction.

* * * * *

Strengthening our communications networks to ensure that all consumers have access to the latest fixed and mobile broadband services is critical to our national security, disaster preparedness and response, and economic growth. To that end, Congress must immediately fill the $3.08 billion funding gap for the Rip & Replace Program. CCA is committed to working with all stakeholders to accomplish the challenging task of securing U.S. networks while maintaining communications services for millions of consumers in rural America. Thank you for the opportunity to testify at this important hearing, and I welcome any questions.