Wednesday, March 23, 2022

Congress Needs to Fix Major Funding Shortfall in Rip & Replace Program

By Michael O'Rielly

For years now, Congress has been appropriately focused on the national security concerns of our nation's communications networks and those nation states or groups seeking to do harm to the American government and its people. From banning specific companies from serving the U.S. market, ensuring the functionality of "Team Telecom", funding removal and replacement of network equipment, and numerous other measures, Congress has sought to minimize key weaknesses and vulnerabilities in these networks. Unfortunately, changes required of the private sector as a result of these measures are proving more expensive than originally anticipated. In particular, applications for reimbursement under the so-called "Rip & Replace" program are now expected to total over $5.6 billion, when only $1.895 billion in Federal funding has been provided for this purpose. Congress can and should promptly fix this, as the failure to do so would undermine a central national security effort and inappropriately leave communications companies holding the bag for these costs.

Meeting Congressional Commitments

The principles established by Congress in the Secure and Trusted Communications Networks Act of 2019 are sound. The applicable House Committee Report notes that "Given the pivotal role that private communications networks serve in connecting U.S. critical infrastructure functions, American networks are appealing targets for foreign adversaries. The United States, therefore, has a clear interest in mitigating threats posed by vulnerable communications equipment and services."[i] A combination of this law and Federal Communications Commission actions effectively does this by requiring a broad swath of certain communications providers' equipment (and services) capable of being abused to the detriment of U.S. national security, particularly that supplied by Huawei and ZTE, be identified and subsequently removed with cost reimbursements paid for by the government. Specifically, Section 4 of the law, as amended, establishes a thoughtful mechanism for smaller providers (those with 10 million or fewer customers) and other key entities (e.g., non-commercial educational institutions, health care providers, and libraries) to remove, replace, and dispose of "communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons". In essence, these providers are obligated to remove untrustworthy equipment and be reimbursed for such costs, while minimizing opportunities for waste, fraud, and abuse.

Indeed, the necessity for the reimbursement program is especially strong. Congress targeted resources to smaller broadband providers that unwittingly purchased cheaper equipment (i.e., Chinese origin), which had the unintended consequence of helping to strengthen the Chinese Government, improve its world influence, and expose U.S. networks for potential manipulation and abuse. As House Energy and Commerce Subcommittee Chairman Michael Doyle stated on the House floor, smaller providers – unlike their larger brethren – "didn't get the same heads-up by our government"[ii] of the risks generated by such equipment. Thus, these entities purchased the troubling equipment without warning and now find

themselves in the unenviable position of being told to remove it. Similarly, Ranking Member Bob Latta stated, “This bill takes into account important concerns we have heard from small, rural providers that were previously unaware of possible security risks when selecting vendors and making purchasing.”[iii] In other words, the U.S. government did not share, either intentionally or by negligence, vital information on potential threat exposures with smaller providers and now seeks their compliance for the equipment removal effort.

To put this in context, Congress and the FCC created the mandates that identified equipment used by certain communications providers be removed. Applicable communications providers are in little position to ignore this requirement and it should not be seen as voluntary. As such, the relevant issue, which was already answered once by the FCC and ostensibly by Congress, is whether cost to smaller providers for conducting this work and replacement equipment should be done *without* sufficient reimbursement. In fact, when considering funding for the Rip & Replace program on the Senate Floor, Senate Commerce Committee Chairman Roger Wicker said, “Let me also make the point that some things are worth paying for, and protecting Americans, protecting our electronic system, our broadband communications from the Chinese-owned Huawei and ZTE is worth paying for.”[iv]

Any lack of additional funding above the $1.9 billion effectively creates a massive unfunded mandate of approximately $3.7 billion, as existing funding will be prorated to recipients. Even though the statute prioritizes funding for very small providers (i.e., those with 2 million or fewer customers), this will not resolve the needs of these providers, necessitating prorated reimbursements at significantly reduced rates. That’s means, smaller providers would be faced with untenable options, including the possibility of going out of business. The result could be even further reduced broadband service in rural areas. In the meantime, these companies are facing extreme uncertainty.

It’s important to note that there is history of Congress increasing initial funding levels after a statute has been passed when it was deemed necessary. Consider the added funding Congress made available under the digital set top box program as part of the analog television conversion process. In that instance, Congress created a two-step funding stream based on consumer demand for the program. However, even with this structure, anticipated demand exceeded funding resources and Congress stepped in to allocate an extra $650 million the program. Likewise, Congress added additional funding as part of the successful Broadcast Incentive Auction. Specifically, the initial costs for the repacking of broadcast stations exceeded the Congressional allotment of $1.75 billion. With more programmatic experience, Congress added an additional $1 billion for the vital reimbursement purposes. In the end, these added funds were essential to accomplishing the Congressional directives contained in the respective statutory provisions.

National Security Needs

The risk of not fully funding the replacement costs for untrustworthy equipment is significant. As House Energy and Commerce Committee Chairman Frank Pallone stated in the requisite House legislative hearing, which helped lead to the statutory provisions, “Communications networks are interconnected and that means that one weak link can harm the whole system. We must help smaller carriers remove suspect equipment for the good of the entire country.”[v] Yet, without sufficient reimbursement funds available, there is a high likelihood that smaller carriers will be simply unable to remove the troubling equipment in any scheduled timeline. Many of these carriers cannot cease operations for a time period to install necessary equipment or conduct the necessary transfer to new equipment while still remaining financially viable. Absent such equipment replacement, the U.S. would consist of a patchwork of upgraded and replaced networks on one hand and those that aren’t able to do so on the other hand. Given the interconnected nature of wired and wireless broadband networks, any system that maintains suspect or untrustworthy equipment makes all networked systems more vulnerable to abuse or potential attack.

To clarify the gravity of this situation, Section 2 of the statute explicitly identifies two threats by not replacing the requisite equipment. First, such network equipment potentially could be used to route or redirect "user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles." This indicates that this suspect equipment is capable of being manipulated for purposes of disrupting user communications or to gain access for some monitoring or perhaps nefarious purpose. The consequences of these scenarios are potentially cataclysmic. For example, disrupting communications could lead to a partial or total shutdown of critical user information, especially during emergencies. Those that have experienced communications blackouts know how damaging this can be. Moreover, allowing a foreign actor to collect and examine user communications could facilitate the building of extensive dossiers on all Americans or obtain the sensitive communications of our elected leaders. Second, the statute identifies the possibility that the untrustworthy equipment could be disrupted remotely. That implies that foreign adversaries could have the means and opportunity from afar and without detection to use weak entry points in the network via this equipment to gain complete control over any connected network. The harms that could come from such an occurrence are immeasurable.

Timing Important for Broadband Access

Complicating the reimbursement program's funding issue is the desire from the legislative and executive branches of the Federal government, as well as state and local officials, to see all Americans have access to broadband. As opposed to those Americans with cost or adoption issues, those without broadband access are disproportionately likely to live in less dense or rural areas of the country. These places tend to be where smaller broadband companies operate and thrive. Furthermore, the smaller providers facing the major Rip & Replace program challenges are likely to be some of the same ones that can bring broadband to unserved Americans.

The problematic Rip & Replace program funding is likely to keep some smaller broadband providers on the sidelines as it comes to expanding out their networks to neighboring areas or expanding to new markets. Such uncertainty may feed into the rates paid for matching capital, when needed, or the willingness of states and other officials to select these providers as winning grantees for new broadband access money. Additionally, it means that applications for broadband network access builds will be more expensive and generate fewer submissions. If policy leaders want to ensure that every American has access to broadband it needs to make sure that those providers likely to bring solutions forward are not financially hamstrung by an underfunded reimbursement program.

* * *

The Rip & Replace program has a sound justification – help protect U.S. national security – and a solid structure. But it lacks the necessary funds to make it effective. That is something Congress can rectify, and I hope it does soon. Absent doing so, we will be left with an under-protected communications network system that leaves Americans more vulnerable to harm and also threatens the viability of rural communications network providers.

---

[i] CRPT-116hrpt352.pdf (congress.gov)

[ii] CREC-2019-12-16-pt1-PgH10282.pdf (congress.gov)

[iii] Ibid.

[iv] CREC-2019-12-19-pt1-PgS7178.pdf (congress.gov)

[v] 2019.9.27.PALLONE. Supply Chain Leg Hearing.CAT .pdf (house.gov)