
Rip & Replace: Bureaucracy and National Security in Critical Infrastructure

Open Access Teaching Case Developed for the Tech for Humanity Pathways Minor

Funded by the Andrew Mellon Foundation

Developed by Erika Heeren-Moon

Background

Telecommunications is a critical aspect of infrastructure in the United States. Historically, the policy conversations surrounding telecommunications include topics like competition (Sawyer, 2019), innovation (Darby & Fuhr, 1998), national security (Carter, et al, 2001), resource allocation, and socioeconomic concerns (Grubestic & Mack, 2016). But what do we mean by telecommunications in the context of infrastructure development? Telecommunications covers a wide range of technologies related to connecting communications between two or more people via a transmitter and a receiver. Currently, these technologies may include broadband internet, mobile wireless networks (e.g., 5G, 6G), wired internet networks, voice-over-internet-protocol (VOIP) systems, radio communications, satellite networks, and devices connected to these networks. Telecommunications *infrastructure* consists of these networks as they connect people, businesses, government services, states, and countries.

Connectivity through telecommunications is a vital component of society in the United States. Our water, energy services, financial services, transportation, and food supply services are largely dependent on the ability of different entities and devices to communicate with each other clearly without interruption (Cybersecurity & Infrastructure Security Agency, 2025). The use of devices to increase the efficiency of essential services has become so commonplace, it is easy to take it for granted. Nevertheless, it is imperative that the networks exist and are accessible by residents in all geographic areas and socioeconomic backgrounds in the United States (Federal

Communications Commission, 2025c). The disconnection of these services can have potentially catastrophic consequences. The capture of sensitive information being sent over these networks also creates a security issue. All of these considerations are impacted by the strength of the supply chain to support this infrastructure with secure hardware and software (Cybersecurity & Infrastructure Security Agency, 2025).

These issues are at the core of telecommunications policy in the United States. A key policy in these efforts is the Universal Service Fund. Universal Service is the “principle that all Americans should have access to communications services (Federal Communications Commission, 2025a).” This policy approach is a prominent element in the establishment of the Federal Communications Commission (FCC), the US federal agency tasked with the regulation of “interstate and international communications by radio, television, wire, satellite, and cable...” (Federal Communications Commission, 2025b).” The FCC oversees the Universal Service Fund (USF), established in the Telecommunications Act of 1996, designed to increase access to telecommunications services. There are four programs under the USF: 1) the Connect America Fund, 2) the Lifeline program, 3) the E-Rate program, and 4) Rural Healthcare Support. This fund is funded through contributions through private telecommunications providers based on their interstate/international revenues (Federal Communications Commission, 2025a). These programs target specific groups in underserved areas across the US and offer a means to make access to telecommunications more affordable through subsidies to the provider companies, to public service centers like schools and libraries, or to consumers themselves (FCC 11-161). The FCC monitors the contributions and disbursements. The fund has contributed to the development of additional infrastructure, particularly in rural and underserved areas.

Case Study

Through subsidies administered via the Universal Services Fund, the FCC has continued to promote the continued development of telecommunications infrastructure in the United States through private providers. As this collaboration with private sector companies progressed, so did the concern of the security in the components of the infrastructure being built. Beginning in 2010, the potential for supply chain deals was broached between Chinese equipment manufacturers and US telecommunications providers. The Chinese companies in question included Huawei and ZTE; and so the purchase of equipment from these two companies in particular became the focus of the “Rip and Replace’ program—although equipment from

other companies is included as well. However, the conversation surrounding security concerns associated with the equipment from these companies continued for several years before the Secure and Trusted Communications Networks Act (otherwise known as "Rip and Replace") became public law in early 2020 (Figure 1).

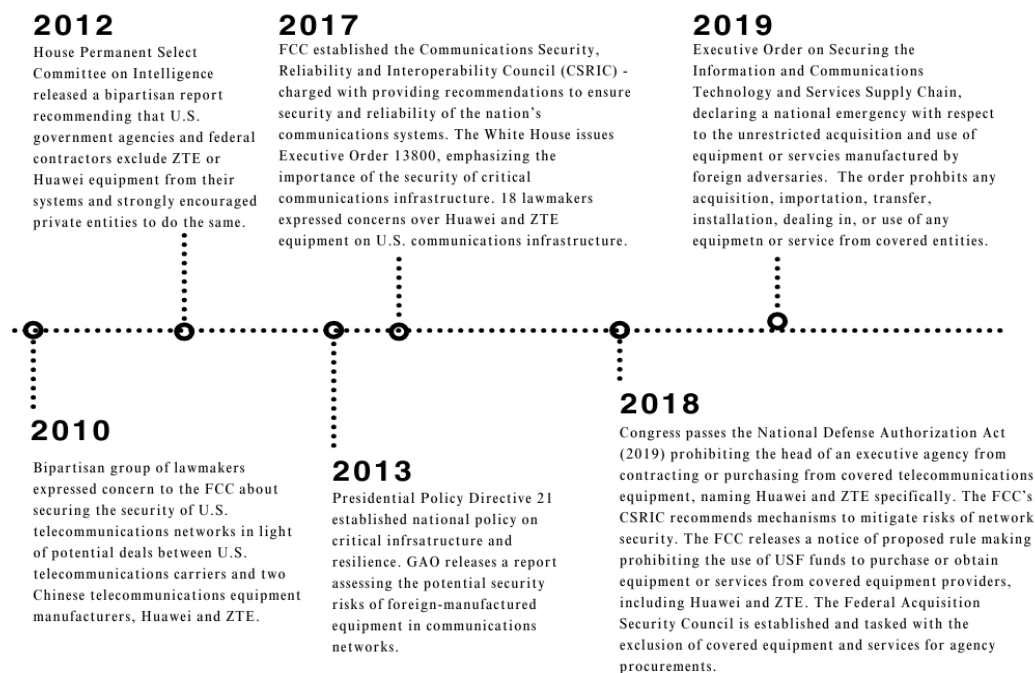


Figure 1: Timeline of Policy Discourse Leading Up to Rip and Replace

The Rip and Replace Program

The Secure and Trusted Communications Networks Act of 2019 establishes “1) a mechanism to prevent communications equipment or services that pose a national security risk from entering US networks, and 2) a program to remove any such equipment or services currently being used in US networks (H.R. 4998).” The bill establishes that federal funds, namely the USF, cannot be used to obtain equipment or services from a company that poses a “national security risk” to critical telecommunications infrastructure. The legislation establishes a fund to provide small telecommunications providers with funds to remove and replace the offending equipment. "Rip and Replace" allocated \$1.9 billion for the FCC to reimburse providers covered under the Act.

In November 2019, the FCC released the First Report and Order addressing the issues

discussed in the (then) pending Secure and Trusted Communications Networks Act of 2019. This order explicitly designated Huawei Technologies Company and ZTE Corporation as companies covered by the Act. The FCC order established the intent of the agency to require all carriers using USF funds to remove equipment from these companies. The order also sought comments from providers and the general public on how to pay for the removal and replacement of the equipment.

After the Secure and Trusted Communications Networks Act of 2019 was passed in March of 2020, the FCC released an order in June 2020 establishing products manufactured by Huawei Technologies Company and ZTE Corporations as a national security risk. The order cites the close connection between the companies and the Chinese Communist Party and military apparatus as justification for the decision. The order also raised the issue of Chinese law requiring the companies to “assist in espionage activities (PS Docket No. 19-352).” Huawei and ZTE both submitted appeals against this order, but they were rejected by the FCC in December of 2020 (PS Docket No. 19-351).

In December 2020, the second report and order from the FCC established and officially adopted the rules for the Secure and Trusted Communications Networks Reimbursement Program. The FCC made the initial estimate of requiring at least \$1.6 billion to reimburse eligible providers. The order required all providers of “advanced communications services” to report whether their networks included any of the covered equipment or services if they were acquired after August 14, 2018 (WC Docket No. 18-89).

In July 2021, the third report and order from the FCC increased the customer eligibility cap for participation in “Rip and Replace” from providers of communications services with a range of two million or fewer customers to ten million or fewer customers. The order also changed the date by which the covered equipment must have been obtained to June 30, 2020. In the case that “Rip and Replace” funding might exceed the \$1.895 billion originally appropriated by Congress, the order enacted a prioritization scheme provided for in the Consolidated Appropriations Act (WC Docket No. 18-89). Shortly thereafter, the FCC released a Small Entity Compliance Guide to assist small businesses in complying with the revised rules (FCC 20-176).

Scope and Scale Challenges: 2022 to 2023

In February of 2022, the FCC announced the release of an online reporting portal for telecommunications providers to report equipment use, removal, and replacement covered under “Rip and Replace.” The reports were required to be submitted no later than May 5, 2022 (DA 22-109). In March 2022, the FCC added equipment and services from three entities, AO Kaspersky lab, China Telecom (Americas) Corp, and China Mobile International USA, Inc. to the list of communications equipment and services deemed a threat to US national security (DA 22-320). In September of 2022, the FCC expanded the list of covered equipment to include PacNet/ComNet and China Unicom (DA 22-979). It is important to note that in the case where the FCC makes additions to the covered list, filers must report any equipment or services obtained 60 days or more after the date they were added to the list (DA 23-167).

The FCC received 181 applications from 96 unique entities for reimbursement after the initial round of applications ended on January 31, 2022. Out of that number, 126 applications from 85 unique applicants were found eligible, which raised the estimated gross cost to \$5.6 billion to remove, replace, and dispose of approximately 24,000 units of equipment from 8,400 locations in the United States and territories (Wireline Competition Bureau, 2023). This was substantially more than the original \$1.9 billion initially made available for the program. While at the time additional funds were not secured, the FCC asserted its commitment to avoiding waste and abuse of the “Rip and Replace” program (DA 22-131).

In July 2023, the FCC’s Wireline Competition Bureau released a report stating that nearly half of the applicants stated that a lack of funding was a key contributor to the barriers they faced in replacing the covered equipment. Other concerns cited included labor shortages and supply chain issues as obstacles to progress toward the “Rip and Replace” goal. Ultimately, at the time of the report, the FCC estimated that 15% of applicants had yet to begin removing the covered equipment, while 83% had made “some progress.” Two percent of applicants reported that they would not begin the work to remove the offending equipment until they received additional funding (Wireline Competition Bureau, 2023). However, the FCC budget request for 2024-2025 did not include additional funds for “Rip and Replace” (Federal Communications Commission, 2024). To accommodate the discrepancy between necessary and estimated funds, the FCC leveraged the prioritization scheme from its initial budget, allocating funding priority to providers with two million or fewer customers. However, applicants only received a prorated support of 39.5% of the reasonable costs to comply as of late November 2024 (DA 24-879).

A Catalyst for Renewal

On December 4, 2024, the FCC released confirmation of reports that foreign actors sponsored by the People's Republic of China had breached at least eight US telecommunications companies as part of an espionage campaign (Federal Communications Commission, 2024). Compromised providers included AT&T, Verizon, and T-Mobile. Hackers targeted lawmakers, members of the US State Department, and people involved in the presidential campaigns of Donald Trump and Kamala Harris (Nakashima, 2024). According to reports, data had been captured through this attack in some cases for over a year (Dou, Cadell, & Menn, 2024).

The vulnerabilities that enabled the Salt Typhoon hackers to attack US telecommunication were attributed to the equipment covered under "Rip and Replace." Equipment removal unfortunately faced a steep barrier in lack of funding. The attacks created a new sense of urgency to continue "Rip and Replace," in order to remove the offending equipment and stop the attacks. To accommodate the discrepancy in necessary funds and allocated funds, Congress authorized the FCC to borrow up to \$3.08 billion from the Treasury Department to fully fund the Secure and Trusted Communications Networks Reimbursement Program through the National Defense Authorization Act (DA 24-1279). With the resurgence of funding, the FCC required providers to submit their annual reports by March 31, 2025 to assess the current and ongoing progress of "Rip and Replace."

Processing Questions

1. How is the Universal Service Fund paid for?
2. What are some examples of how telecommunications infrastructure impacts necessary public services? What would happen if there were a failure in this infrastructure?
3. What programs are funded under the Universal Services Fund, and what public good do they serve?
4. Why were equipment and services manufactured by Huawei Technologies Companies and ZTE Corporation such a key target for the FCC?
5. Does the FCC provide funding through the Secure and Trusted Communications Act of 2019 to offset removal and replacement costs for all providers who have

covered equipment in their networks?

6. The FCC noted a shortage of funding for "Rip and Replace" in early 2022, but funding was not appropriated until 2025 – why?

Thematic Reflection and Discussion

Private Collaboration in Infrastructure Development

The unfolding of the "Rip and Replace" case study is an example of where a disconnect between the private and government sector can lead to costly consequences. The Universal Service Fund was designed to encourage telecommunications providers to increase communications connectivity to underserved areas and demographics. However, the use of equipment from specific companies created a national security issue. This raises questions regarding how a regulatory agency should leverage and manage collaborations with private entities.

Discussion Questions

1. What are the risks of lesser oversight when creating policies to encourage private sector innovation and infrastructure development? What are the risks of too much oversight?
2. Does the method of funding the USF impact how much oversight can/should occur?

Bureaucracy, Innovation, and Security

The risks of installing Huawei and ZTE Corporation equipment in US telecommunications infrastructure was discussed as early as 2010. Yet, there was no regulatory mechanism to restrict the use of this equipment until it had already been widely installed by 2019. The progression of the "Rip and Replace" program provides an example of how knowledge of a risk does not necessarily equate to rapid response to mitigate that risk by the federal regulatory framework.

Discussion Questions

1. What factors may have contributed to the length of time between awareness of the security issue and a regulatory response?
2. How should the US federal government balance the push for innovation and the

need for security?

Risk and Accountability

As the shortage of funding was identified in early 2022, the FCC continued to push for the removal of the offending equipment and services. Even though only 39.5% of the costs were reimbursed to applicants, the FCC emphasized “a recipient’s statutory obligation to complete the permanent removal, replacement, and disposal of covered communications equipment or services exists regardless of the amount of funding it may receive through the reimbursement program pursuant to the Secure Networks Act (DA 24-879).” This decree placed pressure on private entities to accept the burden of costs or risks of breach on their networks. The balance in a public-private collaboration to build infrastructure raises questions regarding who holds the most risk, and who is accountable when something goes wrong, as in the case of the Salt Typhoon breach.

Discussion Questions

1. Who takes on the risk in private sector driven innovation? Who gets the greatest reward?
2. Who should hold the greatest level of accountability in the case of something like a preventable Salt Typhoon breach? Why?

References

- About the FCC. (2025b). Federal Communications Commission. Government Website. Retrieved from: <https://www.fcc.gov/about/overview>
- Bridging the Digital Divide. (2025c). Federal Communications Commission. Government Website. Retrieved from: <https://www.fcc.gov/about-fcc/fcc-initiatives/homework-gap-and-connectivity-divide>
- Carter, A. B. (1989). Telecommunications Policy and US National Security. In R. W. Crandall & K. Flamm (Eds.), *Changing the Rules: Technological Change, International Competition, and Regulation in Communications* (pp. 221–254). Brookings Institution Press. <http://www.jstor.org/stable/10.7864/jj.11589061.10>
- Cybersecurity & Infrastructure Security Agency. (2025). Communications Sector. Government Website. Accessed March 2, 2025. Retrieved from: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector>
- Darby, L., Fuhr, J. (1998). Regulatory perspectives on investment and innovation in US telecommunications. *New Telecom Quarterly*, 6(20). pp. 11-20.

Dou, E., Cadell, C., & Menn, J. (2024). Congress funds removal of Chinese telecom gear as feds probe home router risks. *The Washington Post*. Retrieved from: <https://www.washingtonpost.com/technology/2024/12/19/us-china-telecommunications-defense-rip-and-replace/>

FCC 11.161. (2011). Report and Order and Further Notice of Proposed Rulemaking: In the Matter of a National Broadband Plan for Our Future. Retrieved from: <https://docs.fcc.gov/public/attachments/FCC-11-161A1.pdf>

Federal Communications Commission. (2021). *Small Entity Compliance Guide*. FCC 20-176. <https://docs.fcc.gov/public/attachments/DA-21-1359A1.pdf>

Federal Communications Commission. (2022). Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act. DA-22-320. https://docs.fcc.gov/public/attachments/DA-22-320A1_Rcd.pdf

Federal Communications Commission. (2022). Office of Economics and Analytics and Wireline Competition Bureau Announce the Establishment of the Supply Chain Annual Reporting Portal. DA-22-109. <https://docs.fcc.gov/public/attachments/DA-22-109A1.pdf>

Federal Communications Commission. (2022). Wireline Competition Bureau Announces Applications Filed for The Secure and Trusted Communications Networks Reimbursement Program. DA-22-131. https://docs.fcc.gov/public/attachments/DA-22-131A1_Rcd.pdf

Federal Communications Commission. (2022). Public Safety and Homeland Security Bureau announces additions to the list of equipment and services covered by Section 2 of the Secure Networks Act. DA-22-979. <https://docs.fcc.gov/public/attachments/DA-22-979A1.pdf>

Federal Communications Commission. (2023). Office of Economics and Analytics releases results from initial supply chain annual reports. DA 23-167. <https://docs.fcc.gov/public/attachments/DA-23-167A1.pdf>

Federal Communications Commission. (2024). 2025 Budget Estimates to Congress. <https://docs.fcc.gov/public/attachments/DOC-401057A1.pdf?ref=broadbandbreakfast.com>

Federal Communications Commission. (2024). Streamlined Resolution of Requests under the Secure and Trusted Communications Networks Reimbursement Program. DA 24-879. <https://docs.fcc.gov/public/attachments/DA-24-879A1.pdf>

Federal Communications Commission. (2024). Fact Sheet: Implications of Salt Typhoon Attack and FCC Response. Federal Communications Commission. <https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf>

Federal Communications Commission. (2024). Wireline Competition Bureau and Office of Managing Director Announce Additional Congressional Funding for the Secure and Trusted Communications Networks Reimbursement Program. DA 24-1279. <https://docs.fcc.gov/public/attachments/DA-24-1279A1.pdf>

- First Report and Order: Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89.
<https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf>
- Grubestic, T., & Mack, E. (2016). *Broadband telecommunications and regional development*. Routledge. London; New York, NY.
- H.R. 4998. (2020). Secure and Trusted Communications Networks Act of 2019, 116–124, Retrieved from: <https://www.congress.gov/bill/116th-congress/house-bill/4998>
- Memorandum Opinion and Order: Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs - Huawei Designation, PS Docket No 19-351. <https://docs.fcc.gov/public/attachments/FCC-20-179A1.pdf>
- Nakashima, E. (2024, November 21). Top Senator calls Salt Typhoon “worst telecom hack in our nation’s history.” *The Washington Post*.
<https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/>
- Order: Protecting Against National Security Threats to the Communications Supply Chain through FCC Programs - ZTE Designation, PS Docket No. 19-352.
<https://docs.fcc.gov/public/attachments/DA-20-691A1.pdf>
- Sawyer, L.P. (2019). *US Antitrust Law and Policy in Historical Perspective*. Harvard Business School.
https://www.hbs.edu/ris/Publication%20Files/19-110_e21447ad-d98a-451f-8ef0-ba42209018e6.pdf
- Second Report and Order: Protecting Against National Security Threats to the Communications Supply Chain through FCC Programs, WC Docket. No. 18-89.
<https://docs.fcc.gov/public/attachments/FCC-20-176A1.pdf>
- Third Report and Order: Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89.
<https://docs.fcc.gov/public/attachments/DOC-373481A1.pdf>
- Universal Service. (2025a). Federal Communications Commission. Government Website. Retrieved from: <https://www.fcc.gov/general/universal-service>
- Wireline Competition Bureau. (2023). *Secure and Trusted Communications Networks Reimbursement Program Report*. Federal Communications Commission.
<https://docs.fcc.gov/public/attachments/DOC-390614A1.pdf>