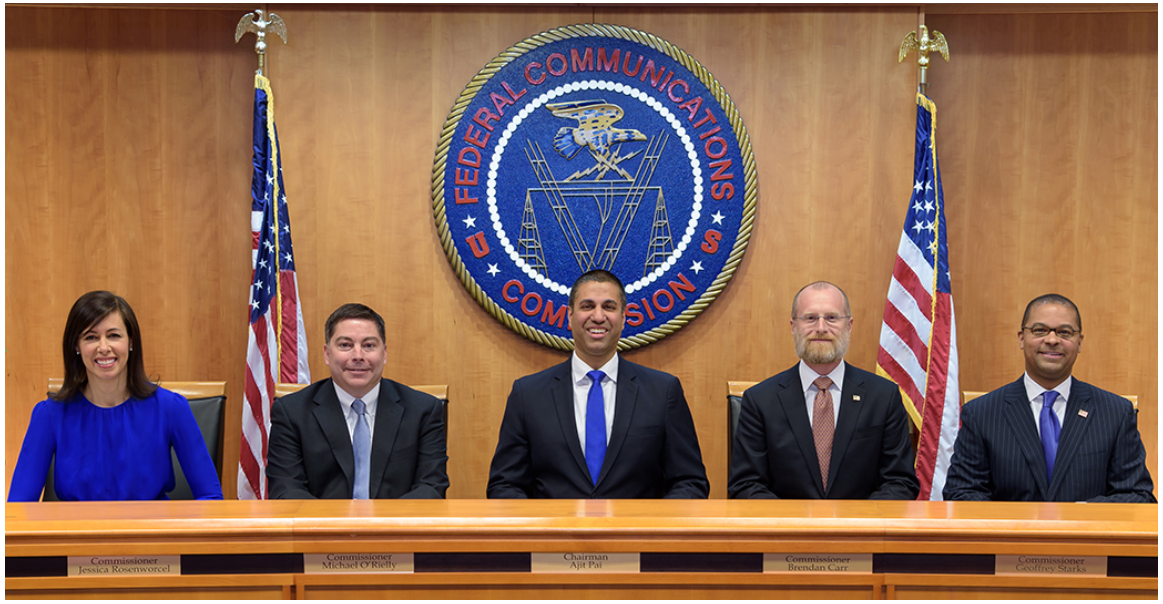
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, FCC 19-121

SOFTWARE AND SUPPLY CHAIN ASSURANCE FORUM
JANUARY 15, 2019

The Federal Communications Commission

- The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the Commission is the federal agency responsible for implementing and enforcing America's communications law and regulations.
- Created in 1934
- Ajit Pai, Chairman



Introduction to the FCC Supply Chain Item

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (FCC 19-121)

- Report and Order, Order, and Further Notice of Proposed Rulemaking
- Adopted November 22, 2019
- Published in the Federal Register on January 3, 2020
- Comments on the Further Notice of Proposed Rulemaking due February 3 and March 3 in WC Docket No. 18-89
- Comments on the initial designations of Huawei and ZTE are due on February 3
    - Huawei Designation – PS Docket No. 19-351
    - ZTE Designation – PS Docket No. 19-352

How did we get here?

- 2012 - House Permanent Select Committee on Intelligence report on the threat from Chinese telecommunications companies operating in and providing equipment to customers in the United States (HPSCI Report)
- 2013 - White House Presidential Policy Directive 21 (PPD 21)
- 2013 – GAO released a report assessing the potential security risks of foreign-manufactured equipment in commercial communications networks and detailing the efforts of the federal government to address the risks posed by such equipment
- 2017 – Executive Order 13800
- 2018 National Defense Authorization Act of 2018
- 2019 National Defense Authorization Act of 2019
- Other Executive Agency Action:
    - 2018 DHS Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force)
    - 2018 SECURE Act – Created the Federal Acquisition Security Council
- 2019 – Executive Order 13873 - Executive Order on Securing the ICT Supply Chain

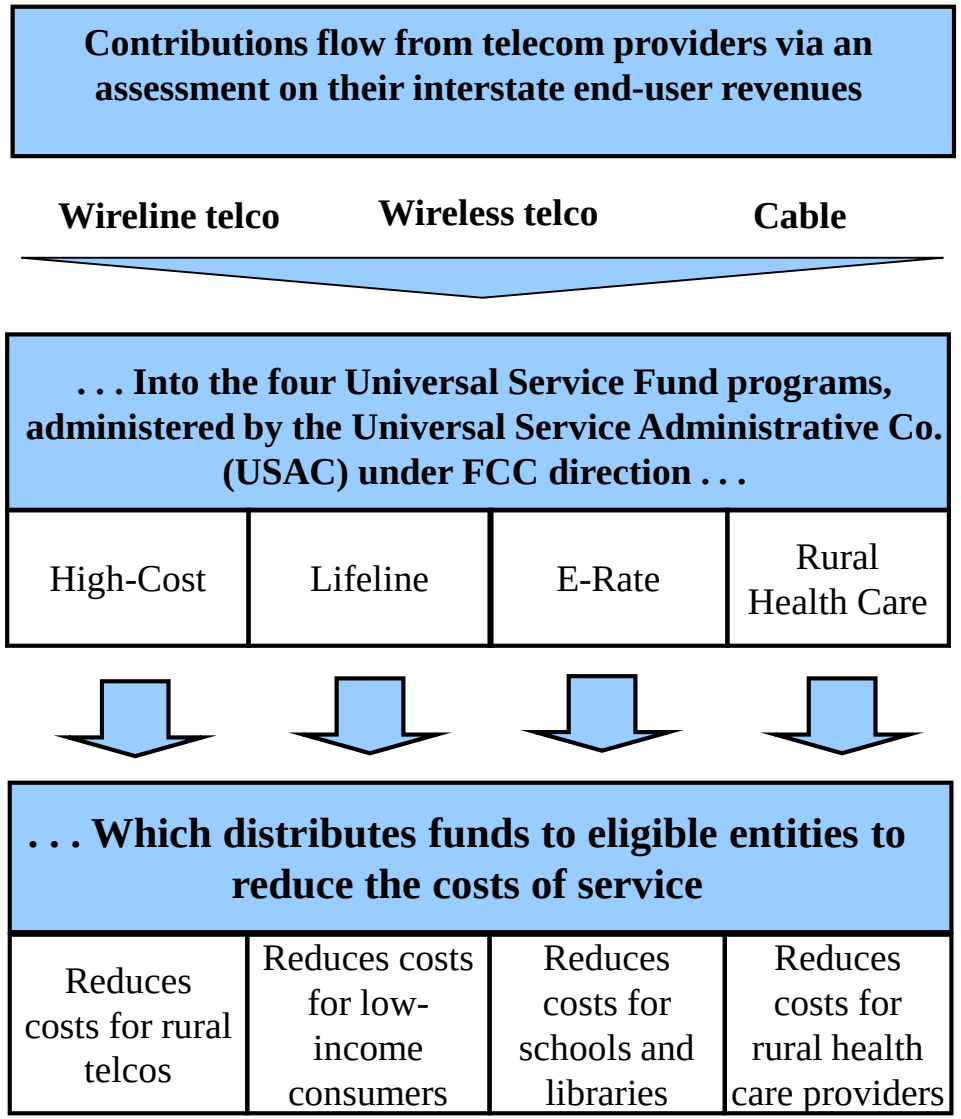
The FCC's Role

- The Communications Act of 1934 includes, among the reasons for the FCC's creation, the purpose of the national defense and for the purpose of promoting safety of life and property through the use of wire and radio communication.
    - The Commission assesses national security and foreign policy concerns in reviewing applications to transfer a spectrum license, a cable landing license, or telephone lines, among other things, when an applicant has reportable foreign ownership.
    - We work closely with sister federal agencies that have additional expertise in these subject areas.
- The FCC previously denied an application from China Mobile, upon the recommendation of Executive Branch agencies, for international section 214 authority on national security and law enforcement grounds.
- Communications Security, Reliability, and Interoperability Council (CSRIC) – a Federal Advisory Council that is currently reviewing, among other things:
    - Mechanisms to best design and deploy 5G networks to mitigate risks to network reliability and security posed by, among other things, vulnerable supply chains
    - Managing Security Risk in the Transition to 5G," and "Managing Security Risk in Emerging 5G Implementation

Universal Service Fund (USF)

"Universal service" – the availability of affordable, reliable telecommunications service throughout the nation – is a fundamental goal of federal telecom law.

Pursuant to Section 254 of the Telecommunications Act of 1996, the FCC established the Universal Service Fund in 1997 to subsidize telecom services for low-income consumers, rural health care providers, schools and libraries, and consumers in high-cost areas.



Federal Communications Commission

2018 Notice of Proposed Rulemaking

APRIL 18, 2018

Supply Chain 2018 NPRM

- Notice of Proposed Rulemaking adopted on April 18, 2018
  - In response to ongoing concerns about the integrity of the communications supply chain, the NPRM proposed and sought comment on a rule to prohibit the use of USF funds to purchase or obtain equipment or services from any communications equipment or service providers identified as posing a national security risk to communications networks or the communications supply chain.
  - Both Huawei and ZTE were cited repeatedly in the Notice as having triggered Congressional concerns regarding the potential for supply chain vulnerability and the possible risks associated with certain foreign communications equipment providers
- October 2018 Public Notice
  - The Commission released a Public Notice seeking comment on the applicability of the 2019 NDAA to the Commission's rulemaking and to the USF programs the Commission oversees. Specifically, the USF National Security Public Notice sought comment on how to interpret section 889 of the 2019 NDAA in light of this proceeding

2019 Report and Order

NOVEMBER 22, 2019

Report and Order

- Adopts 47 U.S.C. 54.9 – no universal service support may be used to purchase or obtain any equipment or services produced or provided by a covered company posing a national security threat to the integrity of communications networks or the communications supply chain
    - USF recipients may not use USF funds to maintain, improve, modify, operate, manage, or otherwise support such equipment or services in any way including upgrades to existing equipment and service.
    - Limited to Eligible Telecommunications Carriers
- Covered Company – a company designated by the FCC as posing a national security threat to the integrity of communications networks or the communications supply chain
- The Report and Order initially designates Huawei and ZTE as covered companies for the purposes of this rule.

Why the Commission Should Act

- The Order finds that Universal Service Funds should not endanger national security.
    - The FCC has authority to place reasonable public interest conditions on the use of USF funds. We find that providing a secure service is part of providing a quality service, which is a requirement of Section 254.
    - National security concerns, and the security of our nation, is an important part of the public interest.
    - Section 201(b) authorizes us to promulgate rules necessary in the public interest to carry out provisions of the act. Promotion of national security is consistent with public interest.
    - Section 105 – the Communications Assistance for Law Enforcement Act – requires the Commission to ensure that interception of call-identifying information effected within switching equipment is activated only pursuant to lawful authorization and the affirmative intervention of an officer of the carrier.

What Does the Rule Impact?

- It applies to any and all equipment or services, including software, produced or provided by a covered company. USF recipients must be able to affirmatively demonstrate that they have not used any funds obtained via the USF to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services provided or manufactured by a covered company.

- The prohibition applies to upgrades and maintenance of existing equipment and services.

- A blanket prohibition best promotes national security, provides the most administrable rule, and eases compliance for USF recipients.
  - Vulnerabilities can be difficult to discover, and malware can be designed and build directly into communications equipment.

- The rule does not prohibit USF recipients from using their own funds to purchase or obtain equipment or services from covered companies, but USF recipients must be able to clearly demonstrate that no USF funds were used.

- Existing multiyear contracts to acquire equipment or services from a covered company will not be exempt from this rule.

Enforcement

- ETCs must certify that they complied with the rule.
- Universal Service Administrative Company (USAC), the organization that administers the Universal Service Fund, will audit USF recipients to ensure compliance.
- USF recipients must be able to affirmatively demonstrate that no universal service funds were used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services provided or manufactured by covered companies.

Designation Process

- The Commission will initially designate a company as posing a national security threat to the integrity of communications networks or the communications supply chain.
- Upon publication of the initial designation in the Federal Register, interested parties will have 30 days to comment on the initial designation.
- If no party opposes the designation, the Commission will release a Public Notice following the 30 day window announcing a final designation.
- If a party opposes the designation, the Commission will review the record and release a final designation no later than 120 after release of the initial designation. The Commission may extend the deadline, but will endeavor not to do so in order to provide certainty to all impacted parties.
- The final determination will be based upon all available evidence.

Huawei and ZTE's Initial Designation

- The item initially designates Huawei and ZTE as covered companies for the purposes of the rule.
- Rationale:
  - There is a substantial amount of evidence about the risks of these two companies.
  - The close ties between the companies and the Chinese government and military.
  - Chinese laws, including the Chinese National Intelligence Law, obligate the companies to cooperate with any request by the Chinese government to use or access their systems, equipment, or network.
  - Chinese intelligence can tamper with products in both design and manufacturing.
  - Authorized access to the telecommunications equipment could be exploited for malicious activity under the guise of legitimate assistance.
  - There are known security flaws in their equipment.
  - End-to-end nature of Huawei's service agreements allow it key access for exploitation.
  - Both companies have a pattern of untrustworthy behavior.
    - China has a "notorious reputation for industrial espionage, for example.
  - This decision was informed by the entire federal government, as well as similar assessments from other countries.

2019 Information Collection Order

NOVEMBER 22, 2019

Information Collection Order

- Collect information to determine the extent to which potentially prohibited equipment exists in current networks and the costs associated with removing such equipment and replacing it with equivalent equipment.
- Focused on Huawei and ZTE and all equipment and services from these companies as used by ETCs.
- Seeks to answer certain questions, including:
  - Do carriers own the equipment?
  - What is the equipment?
  - Cost to purchase and install
  - Cost to remove and replace

2019 Further Notice of Proposed Rulemaking

NOVEMBER 22, 2019

Further Notice of Proposed Rulemaking

- We propose to require as a condition on the receipt of any USF support that ETCs not use or agree to not use within a designated period of time, communications equipment or services from covered companies.
  - Companies would be required to certify as such to receive USF funds.

- We propose to require ETCs receiving USF support to remove and replace covered equipment and services from their network operations.

- Currently propose to limit to eligible telecommunications carriers, but ask whether it should be broader.

- Seek comment on the timelines.

Further Notice of Proposed Rulemaking (con't)

- We propose to establish a reimbursement program to offset reasonable transition costs, and propose to make the requirement to remove covered equipment and services by ETCs contingent on the availability of a funded reimbursement program.

- We propose to make available reasonable replacement costs for the equipment and services produced or provided by covered companies, and we seek comment on this proposal.

- How to fund the proposal?
  - We seek a congressional appropriation.
    - For example, Secure and Trusted Communications Network Act (HR 4998)
  - If not, seek comment on using USF support.
- Comments are due on February 3 and reply comments are due on March 3 in FCC WC Docket 18-89.

Questions?

Justin.Faulb@fcc.gov
202-418-1589