Ensuring Trusted Networks

Ethan Lucarelli
Chief, Office of International Affairs
Federal Communications Commission
United States of America

Note: The views expressed in this presentation are those of the author/presenter and may not necessarily represent the views of the Federal Communications Commission

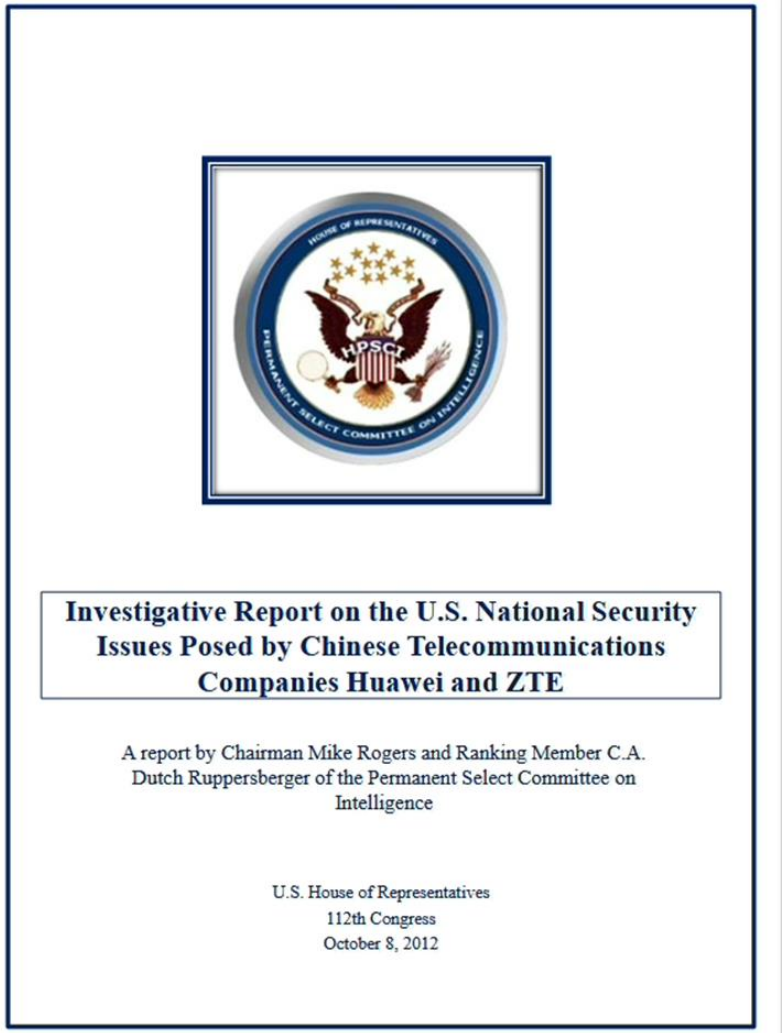
U.S. Federal Communications Commission Strategic Goals, 2022 - 2026

- **Pursue a "100 Percent" Broadband Strategy**
- **Promote Diversity, Equity, Inclusion, and Accessibility**
- **Empower Consumers**
- **Enhance Public Safety and National Security**
- **Advance U.S. Global Competitiveness**
- **Foster Operational Excellence**

None of these goals can be achieved without secure networks!

Protecting the Supply Chain Against National Security Threats

- The Commission, Congress, and the Executive Branch have all recognized that communications equipment and services with poor cybersecurity practices can pose an unacceptable risk to American national security.



Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE

A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence

U.S. House of Representatives
112th Congress
October 8, 2012

Backdrop of Key Actions

1. 2018 National Defense Authorization Act (NDAA)—

Bars the Department of Defense from using "[t]elecommunications equipment [or] services produced . . . [or] provided by Huawei Technologies Company or ZTE Corporation" for certain critical programs, including ballistic missile defense and nuclear command, control, and communications.

2. 2019 National Defenses Authorization Act (NDAA)—

Section 889(b)(1) of the 2019 NDAA prohibits the head of an executive agency from using federal funds to procure or obtain equipment, services, or systems that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system.

Security and the Future of Networks

- Standalone (SA) deployment provides security features not available in 4G
- Network slicing is one of the more well-known security features that prevents Denial of Service Attacks
  - It is not available in 4G, or in 5G Non-standalone (NSA) deployments that mix 5G and 4G components
- Continued evolution of 5G will include Artificial Intelligence (AI)
  - Automatically optimize the operation of the network
  - Detect and protect the network from security attacks

Who do you trust to develop and manage the AI software running on your network?

Backdrop of Key Actions

3. **Secure Networks Act—**

SEC. 2. DETERMINATION OF COMMUNICATIONS EQUIPMENT OR SERVICES POSING NATIONAL SECURITY RISKS.

(a) PUBLICATION OF COVERED COMMUNICATIONS EQUIPMENT OR SERVICES LIST.—Not later than 1 year after the date of the enactment of this Act, the Commission shall publish on its website a list of covered communications equipment or services.

SEC. 3. PROHIBITION ON USE OF CERTAIN FEDERAL SUBSIDIES.

(a) IN GENERAL.—

(1) PROHIBITION.—A Federal subsidy that is made available through a program administered by the Commission and that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service may not be used to—

(A) purchase, rent, lease, or otherwise obtain any covered communications equipment or service; or

(B) maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained.

SEC. 4. SECURE AND TRUSTED COMMUNICATIONS NETWORKS REIMBURSEMENT PROGRAM.

(a) IN GENERAL.—The Commission shall establish a reimbursement program, to be known as the "Secure and Trusted Communications Networks Reimbursement Program", to make reimbursements to providers of advanced communications service to replace covered communications equipment or services.

FCC Actions to Secure the Nation's Networks

The FCC is:

- **Taking direct action to limit presence of equipment from untrusted vendors in US networks.**
- **Moving fast to speed the way for trustworthy innovation.**
- **Collaborating across government, with industry, and with partner nations on a multifaceted, strategic approach to protect our networks from all threats.**

Key Actions by the FCC

- **November 2019: First Report and Order**
  https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf

- **December 2020: Second Report and Order**
  https://www.fcc.gov/document/fcc-adopts-rules-secure-communications-networks-and-supply-chain-0

- **March 2021, March 2022, September 2022: Publication of FCC Covered List**
  https://www.fcc.gov/supplychain/coveredlist

- **November 2022: Equipment Authorization Report and Order**
  https://www.fcc.gov/document/fcc-adopts-rules-secure-communications-networks-and-supply-chain-0

2019 Secure Network Act and "Covered List"

- Following passage of the Secure Networks Act of 2019, the Commission issued multiple orders seeking to protect against national security threats to the communications supply chain, including by barring communications service providers from using Universal Service funding to purchase, obtain, maintain, improve, modify or otherwise support any equipment or services on the "Covered List."

2019 Secure Network Act and "Covered List"

The "Covered List" currently includes all telecommunications equipment produced or provided by Huawei or ZTE, as well as all video surveillance and telecommunications equipment produced by Hytera Communications Company, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company.

The "Covered List" also includes telecommunications services provided by China Mobile International USA, China Telecom Americas, China Unicom Americas, and Pacific Networks/ComNet.

Two Requirements for Inclusion in the Covered List

(b) The Commission shall place on the list published under subsection (a) any communications equipment or service, if and only if such equipment or service— (1) is produced or provided by any entity, if, based exclusively on the determinations described in paragraphs (1) through (4) of subsection (c), such equipment or service produced or provided by such entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(**2) is capable of**— (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles;

(B) causing the network of a provider of advanced communications service to be disrupted remotely; or

(C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(c) Reliance on certain determinations In taking action under subsection (b)(1), the Commission shall place on the list any 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 based solely on one or more of the following determinations:

(1) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41.

(2) A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain).

(3) The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918).

(4) A specific determination made by an appropriate national security agency.

Secure and Trusted Communications Networks Reimbursement Program (SCRP) ("rip & replace")

- Pursuant to the Secure and Trusted Communications Networks Act, the FCC has established a program to **remove, replace, and dispose of "covered equipment" already deployed in U.S. networks**:
  - FCC will reimburse eligible providers for reasonable expenses incurred in removing, replacing, and disposing of equipment (Cost Catalog)
  - Providers of advanced communications service with 10 million or fewer customers are eligible
  - Congress has appropriated $1.895 billion in funding
- Filing window = Oct. 29, 2021 to Jan. 28, 2022 (around 180 applications).
- **Annual reporting of any acquisition of covered equipment:** Providers of advanced communications service will have to annually report the existence of equipment or services included on the Covered List in their networks.

Equipment Authorization Proceeding

In November 2022, the FCC adopted a Report and Order to further the Commission's goal of protecting our communications networks and supply chains from equipment and services that pose an unacceptable risk to national security by amending our rules related to equipment authorization and competitive bidding.

Equipment Authorization Report and Order

The Report and Order:

- Prohibits “covered” equipment from obtaining an equipment authorization through either certification procedures or Supplier’s Declaration of Conformity procedures

- Requires that each applicant for equipment certification attest in its application that the particular equipment for which it seeks certification is not “covered” equipment

FCC Investigation of Open RAN

- Open RAN Notice of Inquiry (NOI) (March 2021)
- Open RAN Solutions Showcase (July 2021)
- Ongoing discussions with Open RAN innovators and interested service providers
- The FCC’s Communications Security, Reliability, and Interoperability Council VIII (CSRIC VIII) is providing recommendations to promoting security, reliability and interoperability of open RAN equipment and explore what new efforts can be taken to ensure secure-RAN deployments.

FCC Denial of Authority Based on National Security Considerations

- In May 2019, the Commission denied the application of **China Mobile USA** for an authorization to provide international telecommunications services between the United States and foreign destinations.
  - The Commission concluded that, due to a number of factors related to China Mobile USA's ownership and control by the Chinese government, grant of the application would raise substantial and serious national security and law enforcement risks that cannot be addressed through a mitigation agreement.
  - Based on the record, the Commission found that China Mobile USA had not demonstrated that its application for international telecommunications services authority was in the public interest.
- On June 17, 2020, the relevant Executive Branch agencies (security and economic) recommended that the Commission partially deny a submarine cable landing license application for the Pacific Light Cable Network, on national security grounds.

FCC Revocation of Authority Based on National Security Considerations

FCC taking action to ensure that foreign telecommunications companies that obtain or seek access to U.S. markets do not present national security threats

- **In October 2021 and January 2022, the FCC revoked domestic authority and revoked/terminated international authority for China Telecom Americas and for China Unicom Americas, respectively, to provide domestic interstate and international telecommunications services within the U.S.**

- **In March 2022, the FCC revoked domestic authority and revoked and terminated international authority for Pacific Networks Corp. and its wholly-owned subsidiary, ComNet (USA) LLC, to provide domestic interstate and international telecommunications services within the U.S.**

Security and the Future of Networks

- Network operators consider deploying standalone (SA) v. non-standalone (NSA) systems. A standalone deployment provides security features not available in 4G, which uses a non-standalone deployment.

- Network slicing is one of the more well-known security features that prevents Denial of Service Attacks.

  It is not available in 4G, or in 5G non-standalone deployments that mix 5G and 4G components.

- Continued evolution of 5G will include Artificial Intelligence (AI) to:
  - automatically optimize the operation of the network
  - detect and protect the network from security attacks

Whom do you trust to develop and manage the AI software running on your network?

Thank You