Agenda

- Bureau Overview
- Emergency Communications
- CSRIC
- Cyber and Network Resiliency
- ERIC
- Key Issues
• Bureau Established in 2006

• Primary Mission Essential Function

  "Ensure the continuous operation and reconstitution of critical communications system and services."

• Strategic Goal

  "Communications during emergencies and crisis must be available for public safety, health, defense, and emergency personnel, as well as all consumers in need. The Nation's critical communications infrastructure must be reliable, interoperable, redundant, and rapidly restorable."
PSHSB Key Priorities

- Public Safety
- COOP/COG
- Outreach
- Critical Infrastructure
- Emergency Response
- Emergency Preparedness
Public Safety Spectrum
Core of the Public Safety Network Using Public Safety Dedicated Spectrum
10 MHz

Provides nationwide interoperable coverage for day to day operations and most emergencies, guaranteed access and hardened against disasters and power outages

700MHz Commercial Networks
Priority access and roaming
Up to 60 MHz

Provides access to additional capacity during major emergencies, and increased network resiliency and redundancy if the public safety system goes down or is not available

Distributed Antenna System and Microcells
In-building and underground coverage
Improves localized performance

Coverage inside buildings and capacity for high pedestrian density can be provided by in-building solutions

Deployable Equipment
Cellular on Wheels and Externally Mounted Antennas on Public Safety Vehicles

Boosts capacity for the worst emergencies and in rural areas

For exceptional times and places when public safety and commercial infrastructure is insufficient

Nationwide, 99% population coverage from dense cities to rural counties

Public Safety Broadband Network
The Emergency Response Interoperability Center

- Created in April 2010 with the mission of establishing a technical and operational framework that will ensure nationwide operability and interoperability in deployment and operation of the 700 MHz public safety nationwide broadband wireless network.
ERIC Public Safety Advisory Committee

Responsible for assisting ERIC with the following policy objectives:
(1) the adoption of technical and operational requirements and procedures to ensure a nationwide level of interoperability;
(2) the adoption and implementation of requirements and procedures to address operability, roaming, priority access, gateway functions and interfaces, the interconnectivity of public safety broadband networks and other matters related to the functioning of the nationwide public safety broadband network;
(3) the adoption of authentication and encryption requirements for common public safety broadband applications and network use;
(4) the coordination of ERIC’s policies with other entities, including other federal agencies; and
(5) such other policies for which ERIC may have responsibilities from time to time.
Emergency Communications

- National Security Leadership
- National Security Posture and U.S. Population Attack Warning
- Public Health, Safety and Maintenance of Law and Order
- Public Welfare and Maintenance of National Economic Posture

Organizations that support one or more of the listed National Security/Emergency Preparedness (NS/EP) mission areas, qualify to use priority services.

(* EOP: Executive Office of the President)
Priority Service Programs

- **Telecommunications Service Priority** – A FCC program that authorizes NS/EP organizations to receive priority treatment for vital voice and data circuits or other telecommunications services.

- **Wireless Priority Service** - A priority calling capability that greatly increases the probability of call completion during a NS/EP event over a wireless networks.

- **Government Emergency Telecommunications Service** - Provides emergency access and priority processing in the local and long distance segments over a wireline network.
The Communications Security, Reliability and Interoperability Council

Provides recommendations to the FCC related to facilitating:
(1) the security, reliability, operability and interoperability of public safety communications systems;
(2) the security, reliability, operability, and interoperability of wireline, wireless, satellite, cable, and public voice and data networks; and
(3) the security and reliability of broadcast and Multichannel Video Programming Distribution facilities.

Recommendations will address:
(1) ensuring the availability of communications capacity during natural disasters, terrorist attacks, or other events that result in exceptional strain on the communications infrastructure; and
(2) ensuring and facilitating the rapid restoration of communications services in the event of widespread or major disruptions.
The National Broadband Plan’s recommendations for cybersecurity:

- FCC should issue a cybersecurity roadmap;
- FCC should expand its outage reporting requirements to broadband service providers;
- FCC should create a voluntary cybersecurity certification program; and
- FCC and DHS should create a cybersecurity information reporting system.
The National Broadband Plan’s recommendations for protecting critical infrastructure:

- FCC should explore network resilience and preparedness;

- FCC and NCS should create priority network access and routing for broadband communications; and

- FCC should explore standards for broadband communications reliability and resiliency.
PSHSB Key Issues

- 700 MHz Public Safety Broadband Network
- 800 MHz Rebanding
- UHF/VHF Narrowbanding
- Emergency Alerting
- Outage Reporting Requirements
- Wireless E911
- NG911
- Cyber Security
- Communications Assistance for Law Enforcement Act
- Travelers’ Information Stations
Thank You!
Questions?
Jennifer Manner
Jennifer.Manner@fcc.gov
202-418-3619