The Innovation Band

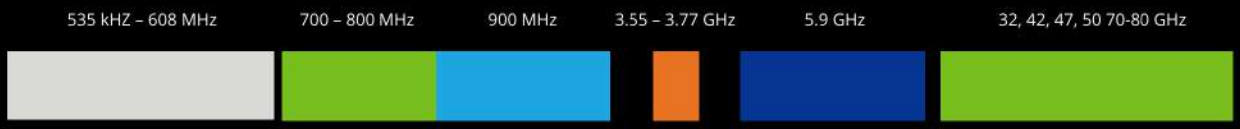
What Citizens Broadband Radio Service Means for America

Government mobility is about to get a massive upgrade. That's because in late 2018, the Federal Communications Commission (FCC) finalized rules for unlocking the 3.5GHz band of spectrum known as the Citizens Broadband Radio Service (or CBRS).

Government Business Council (GBC), the research arm of Government Executive Media Group, has partnered with Ruckus Networks to create an immersive infographic detailing what CBRS is all about and what it means for the federal government in 2019 and beyond.

What is Citizens Broadband Radio Service?

Hover over the radio wavelengths below to understand their use.



Also called the 'innovation band', the 150 MHz of wireless spectrum is now completely dedicated toward CBRS use.

For years, spectrum has provided government, particularly the Department of Defense (DoD), with the wireless support it needs to manage and safeguard satellite, radar, and military communications.

Spectrum is already a scarce resource that citizens and government alike depend on for their daily wireless needs.

CBRS marks an evolutionary milestone to the framework of shared spectrum: by deploying a three-tier model, it allows for spectrum sharing, allowing general authorized users to deploy private LTE based solutions of their own.

The three-tier model protects incumbent users in the band, such as satellite, radar, and other priority operators. The FCC is expected to authorize complete commercial CBRS spectrum availability in Q3 2019. Essentially, if the higher tiers aren't using all of the spectrum in a given time, general authorized access users are free to use that spectrum.

Indeed, CBRS is a perfect vehicle for unleashing the power of private wireless LTE. Compared to WiFi, LTE networks offer greater bandwidth capacity, lower latency, more predictability, and improved security with built-in over-the-air encryption.

What is the three-tier model for CBRS?

Tier One: Incumbents

Incumbent Access users include authorized federal users, grandfathered Fixed Satellite Service earth stations, and, for a limited time, Grandfathered Wireless Broadband Licensees in the 3650-3700 MHz portion of the band. These users will be protected from harmful interference from Priority Access and

General Authorized Access (GAA) users.

Tier Two: Priority Access

The Priority Access tier consists of Priority Access Licenses (PALs) that will be assigned using competitive bidding within the 3550-3650 MHz portion of the band. Each PAL is defined as a renewable authorization to use a ten megahertz channel within a county for ten years. Up to seven total PALs may be assigned in any given county with up to four PALs going to any single applicant.

Tier 3: General Authorized Access

The GAA tier is licensed-by-rule to permit open, flexible access to the band for the widest possible group of potential users. GAA users are guaranteed access to a minimum of 80MHz and are permitted to use any portion of the 3.5 GHz band not assigned to a higher tier user and may also operate opportunistically on unused Priority Access channels.

Why Expand CBRS to Federal Agencies?

The federal government's data needs have reached a tipping point, all but ensuring that CBRS will be the top mobile priority in 2019. A GBC survey of federal employees in late 2018 shows unprecedented appetite for mobility and wireless fidelity:

56%

use one or more wireless mobile devices to carry out their work duties

72%

said their work-issued mobile devices were essential for using on the job

51%

said their ability to be productive is considerably or extremely dependent on wireless access

78%

said they had no familiarity or knowledge of CBRS prior to taking the survey

The government's wireless usage is only going to increase as the number of mobile devices and network-connected touchpoints expand in scale and volume. Traditional WiFi can't accommodate these trends by itself, and providing coverage via existing wireless models can't guarantee secure, uninterrupted service when users require it.

Private Wireless Networks

Improved Mobility

Decreases Security Risks

What does this look like in action?

Ironclad Security

Intelligence agencies like the CIA, NSA, and NGA could provision LTE network access that is completely secure and contained to their agency *without* having to relay data back through mobile carriers and thirty party providers.

Unprecedented Mobility

Working with CBRS providers, agencies such as Department of Transportation and Homeland Security could equip their vehicles with LTE gateways, providing a level of mobility not available via traditional WiFi.

Unleash the Internet of Things

CBRS lets agencies truly own their IoT device management. Imagine DoD military outposts augmenting their networks with surveillance devices for round-the-clock visibility, or Department of Energy personnel receiving real-time feeds of electrical grid infrastructure that magnify changes in the system.

Privacy Guaranteed

By harnessing LTE access through CBRS, General Services Administration could help agencies procure Push-to-Talk phones or mobile devices specifically tailored to that agency's mission needs, ensuring total privacy of communications.

Ensure network integrity

‹

Government IT leaders and other agency stakeholders will have to architect necessary security tools and protocols to ensure protection in the new CBRS-based networks

›

ensure protection in the new CBRS based networks.

Get Your Agency Started with the Following Resources

EXPLORE GBC'S RESEARCH

WATCH THE VIDEO RECAP

CONSULT AN INDUSTRY PARTNER