Government Business Council

Citizens Broadband Radio Service

Top 5 Things You Should Know

Underwritten by: RUCKUS an ARRIS company

The rise of high-speed wireless access redefined the mission potential of public servants in the 21st century. While many advancements can trace their origin to the convenience created by WiFi services, new legislation finalized by the Federal Communications Commission (FCC) in 2018 now ensures that mobile spectrum broadband will play a major role in providing the secure coverage agencies need.

Here are five things you should know about Citizens Broadband Radio Service (CBRS), and why it spells big changes for the years ahead.

1 What does it do?

CBRS is the answer to a problem: what to do when spectrum is limited, but data demands continue to grow year over year?

Ubiquitous connectivity and wireless access are now integral to 21st century life, with over 75% of Americans in possession of smartphones and tablets as of 2018 — *doubling* ownership levels recorded just 7 years ago.

The wireless revolution is taking place in government too, where employees are increasingly called on to deliver results against a changing, fast-moving, mobile mission-scape.

CBRS capitalizes on such mobility by preserving 150 MHz of wireless spectrum for government agencies, companies, and citizens to deliver LTE services *without* requiring a license.

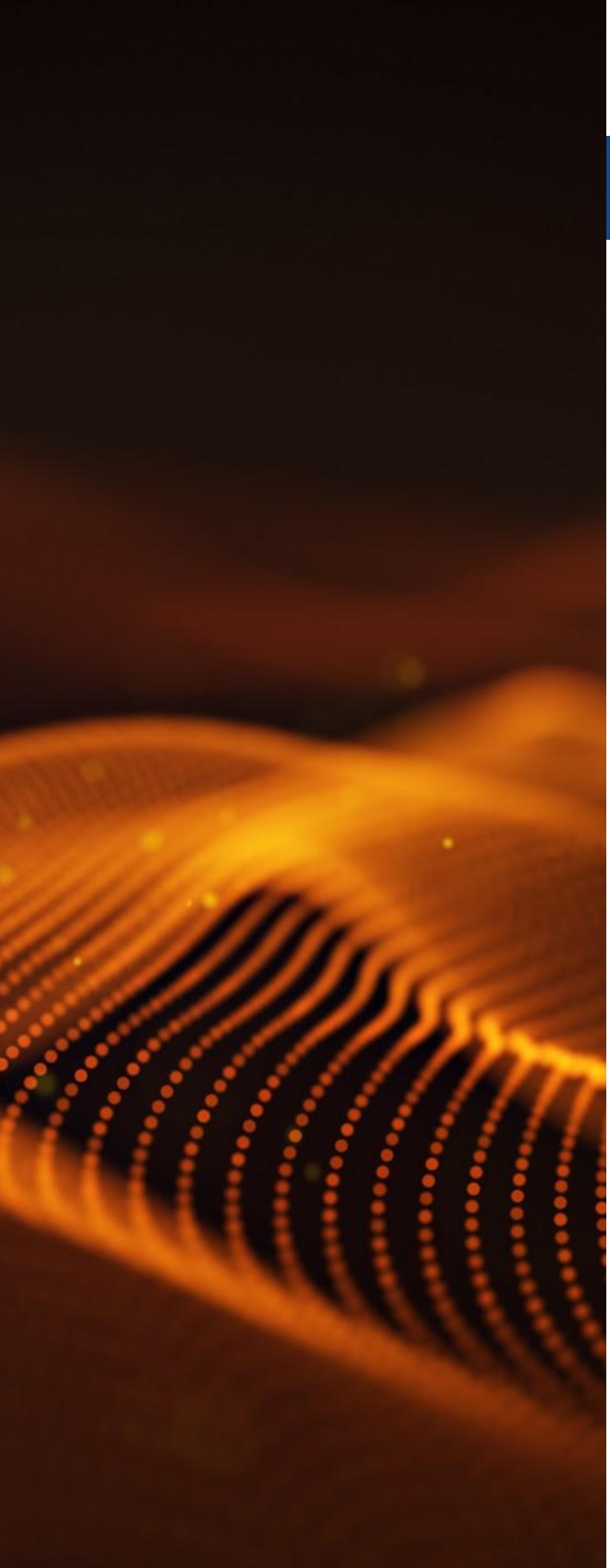
Instead of auctioning off this spectrum to the highest bidder, the FCC established an innovative operating model to ensure that spectrum can be shared, allocated appropriately, and thereby benefit all parties.[1]

What this means is that incumbent users like DoD can keep the spectrum needed to maintain satellites, radar, and military communications. However, it also means that other agencies can now come on board, installing their own private closed networks to enable indoor cellular coverage, support wide-area surveillance, and safeguard critical communication channels across the enterprise.

2 Deploys at WiFi speed

One of the most striking features about CBRS is that it allows private LTE cellular (or 4G) to be deployed just as quickly as WiFi. For years, WiFi was the more viable option, able to be set up and configured in a matter of hours unlike private LTE networks that could take weeks to months to set up.

That's now changed with the introduction of CBRS. By unlocking the 3.5 GHz band, FCC has made it possible for government agencies to deploy their own private wireless networks in mere hours, providing 'campus connectivity' to an increasingly mobile workforce.



It's what the Internet of Things has been waiting for 3

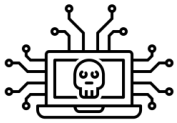
Three years ago, the number of Internet-connected devices surpassed the total human population. By 2020, experts predict this Internet of Things (IoT) will encompass over 20 billion devices.[2]

The federal government's current network infrastructure is unprepared for this kind of magnitude. As devices grow in number and extend mission mobility, agencies will require quicker, more comprehensive coverage than WiFi deployments allow: because it is unlicensed, WiFi is prone to congestion and interference from a surge of users.

But under CBRS, DoD operators can effectively create 'smart bases' for their military, using private LTE spectrum to house and monitor their entire arsenal of IoT devices. CBRS can advance the Department of Transportation's mission to leverage IoT sensors for better assisting travelers with disabilities.[3] And CBRS can aid the Department of Energy's goal of building a smart grid that informs proactive maintenance of critical infrastructures.[4]

> ***We have a pretty diverse mission set and they all use mobile differently. They all want it out in the field, and they need to have that data right there with them.***
>
> - Brian Varine, Chief of Cyber Threat Intelligence, Department of Justice

4 *It's secure and stable*



The U.S. government may be the world's largest target of cybersecurity attacks so it's no surprise that federal agencies reported more than 35,000 cyber 'incidents' to the Homeland Security department in 2017 alone.[5]

Concerningly, many of these incidents resulted from employee violations of online activity and use of unauthorized channels to secure information. Lacking a resilient, stable network infrastructure, employees can be tempted to use personal WiFi on their devices and inadvertently leave their agencies open to attack.

With CBRS, this isn't a concern because the private network ensures exclusive access to users within a defined geographical limit. That's especially useful for agencies housing medical facilities to treat the wounded — if WiFi or legacy systems fail, CBRS spectrum ensures these patients can receive uninterrupted care through a network of connected medical providers.

5 It's backed by the world's leading wireless providers

CBRS is backed by many of the nation's leading wireless service providers and carriers. The **CBRS Alliance** is working with government agencies and the FCC to pave the way for shared spectrum access in government, and its collective membership of leading experts ensures that CBRS will provide agencies a pipeline to innovative technologies and smart partnerships in the years ahead.[6]

Under this arrangement, government agencies get the best of both worlds: they get the control and visibility that comes with building private LTE 4G networks to secure their most prized assets, while benefiting from commercial technology that bypasses the hassle of standing up costly, proprietary infrastructures from scratch.

> ***The United States is involved in a global race for supremacy over the next generation wireless technology. First-mover nations will gain enormous increases in gross domestic product, productivity, employment and innovation, as well as be able to drive future wireless developments.***
>
> - Michael O'Rielly, FCC Commissioner

ENDNOTES

1. Federal Communications Commission: "3.5 GHz Band / Citizens Broadband Radio Service." https://www.fcc.gov/wireless/bureau-divisions/broadband-division/35-ghz-band/35-ghz-band-citizens-broadband-radio

2. *The Conversation*: "Internet of Things: when objects threaten national security." May 29, 2018. http://theconversation.com/internet-of-things-when-objects-threaten-national-security-96962

3. Federal Transit Administration: "Report to Congress on Internet of Things." Feb 2017. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/research-innovation/60436/ftareportno0099.pdf

4. Department of Energy: "Internet of Things-enabled Devices and the Grid." June 1, 2017. https://www.energy.gov/articles/internet-things-enabled-devices-and-grid

5. *Nextgov*: "Agencies Faced More Than 35,000 Cyber Incidents in 2017, Watchdog Says." Dec 18, 2018. https://www.nextgov.com/cybersecurity/2018/12/agencies-faced-more-35000-cyber-incidents-2017-watchdog-says/153659/

6. CBRS Alliance. https://www.cbrsalliance.org/

Government Business Council

RUCKUS™ an ARRIS company

About Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis

Report Author: Daniel Thomas

About Ruckus

Ruckus Networks, an ARRIS company, is redefining connectivity around the globe. Ruckus' high-performance network infrastructure provides secure, reliable access to data, applications and services no matter how tough the environment. Ruckus innovates across wired and wireless technology to modernize federal networks and deliver mission success. When connectivity really matters, the federal government turns to Ruckus.

Learn more at www.ruckusnetworks.com