carahsoft | verizon | ERICSSON | leidos

WEBINAR DIGEST

In-Building Connectivity for Return-to-Office Federal Workforces

Enabling seamless, secure, and scalable solutions

Federal employees are returning to the office under new mandates, but while the desks and spaces may look the same, connectivity expectations have changed dramatically. Following years of remote and hybrid work, employees now demand the same seamless, secure, and high-performance connectivity in federal offices that they've grown accustomed to at home or on the move.

> **"How do you create and maintain that same experience? That mobility aspect of still being able to move around, have data at your fingertips, and still have continuity of conversation," asked Lamont Copeland, Senior Director for Federal Solutions Architecture at Verizon.**

Though the shift presents challenges, it also offers a rare opportunity for federal agencies to leapfrog outdated infrastructure to close long-standing technology gaps needed for a modern, efficient, and secure workplace. Achieving that outcome requires a layered, wireless-enabled approach, grounded in user needs and strengthened by public-private collaboration.

This white paper brings together insights from leaders at Verizon, Leidos, and Ericsson to explore what it takes to modernize in-building connectivity for federal environments.

A new reality: managing sky-high expectations with outdated infrastructure

Today's federal workforce expects more than just a return to business as usual. Employees want intuitive, fast, and secure digital experiences from the moment they enter the building. "People got used to the coffee shop experience. Being able to go and work wherever they want," said Scott Robohn, Consulting CTO at Carahsoft.

These same expectations aren't just for those returning to the office but for those who are entering the federal workforce for the first time. "Last year we had a conversation about that seamless experience for new recruits in the Armed services," Robohn shared. "Young men and women coming in and wanting that experience on their phone just like they have it at home."

> **Unfortunately, many federal offices were already lagging behind even before the pandemic, and years of underuse only deepened the divide. Kevin McFadden, Networks Practice SME at Leidos, explained that "the technologies in the wiring closet, the technologies on the desktop, have a very finite lifespan, in many cases just three to five years." When this limited cycle is paired with two to five years of sitting dormant, much of the infrastructure has reached or exceeded obsolescence, delivering less utility and creating operational risk.**

As McFadden concluded, "now you have office spaces burdened by technology debt, compounded by years of inaction" — a reality that government leaders and decision makers must confront to preserve mission readiness and effective public service. Managing this technical debt requires more than the old way of thinking. Mark DeVol, VP of Federal Services at Ericsson, on the Enterprise Wireless Solutions Business Group, said, "The way we really have to address this return to office, this technology gap is a shift in mindset on the approach - not as a static wired experience, but as a dynamic, layered approach to meet modern needs."

What’s standing in the way?

Even as agencies recognize the value of reliable in-building connectivity as employees return to office, many face persistent obstacles making seamless coverage difficult. From physical barriers to financial limitations, the path to modern networks is rarely straightforward.

Some of the key obstacles agencies encounter as they seek to bring office environments up to today’s standards include:

- Aging infrastructure: Thick concrete walls, legacy cabling, and outdated materials inhibit signal penetration.
- Budget constraints: Agencies are asked to modernize without significantly increasing costs.
- Operational disruptions: Renovations can cause downtime and interfere with mission operations.
- Fragmented approaches: Disconnected systems and vendor silos make holistic upgrades difficult as the norm.

The case for wireless and layered connectivity

With these new, heightened expectations, it’s time to consider “a different way of thinking about how federal agencies deliver services out to that end user,” said Copeland. That means embracing a layered approach that combines wired, wireless, and satellite solutions, “to come up with the right solutions, the right plans, the right way to attack problems” based on mission requirements.

> **“We have to look at all these different communications technologies as viable options,” DeVol agreed. “It can’t be an all-or-none situation.”**

This approach is especially critical in complex federal environments where legacy infrastructure and physical constraints often limit traditional wired solutions. In use cases like smart warehousing or DoD material handling systems, persistent, high-performance wireless connectivity can become a safety imperative. “If I have material handling systems or robots that need persistent connectivity, so they don’t roll over the humans, you need persistent, secure connectivity like 5G,” noted Robohn .

Why wireless matters

As agencies rethink how to deliver mission-critical connectivity to employees returning to office, wireless connectivity brings a set of advantages that are difficult to match with wired solutions alone. “Leveraging wireless technologies to get after these and potentially get over that hurdle is really going to be key.” The benefits can reduce costs and minimize disruptions while providing the flexibility federal workforces need as mission demands evolve.

Wireless brings unique advantages:

- Rapid deployment: Avoids costly and disruptive fiber pulls.
- Scalability: Supports future capacity needs without major retrofits.
- Mobility: Enables seamless movement across devices and locations.
- Security: Modern 5G networks include encryption and Zero Trust frameworks.

Security as a foundation, not an afterthought

Connectivity without security is a liability, especially in federal environments where sensitive missions depend on uninterrupted access to data and applications. Employees returning to the office expect the same seamless, fast experience in office as they've had at home, but as Copeland emphasized, "it also must be done in a secure manner."

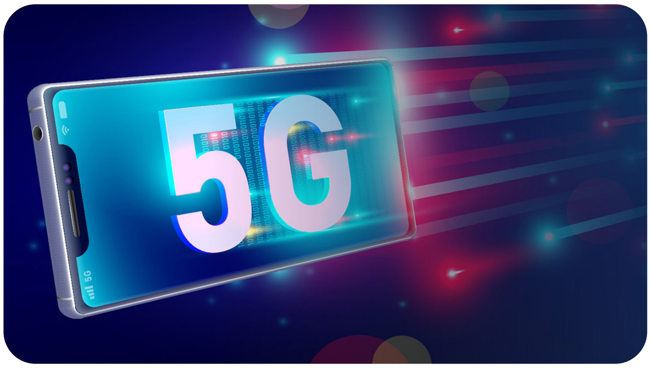
That means building security into every layer of connectivity from the start, not bolting it on afterward. Agencies can no longer rely on static, perimeter-based defense. "It used to be trust but verify. Now with networks, it's verify then trust," explained DeVol. This shift has accelerated with the adoption of Zero Trust principles, supported by modern capabilities like encrypted tunneling, multi-factor authentication, and FedRAMP High-compliant solutions that secures data in transit and at rest.

A layered approach is particularly necessary for federal networks that extend beyond traditional office walls, like supporting National Guard units in the field or mission-critical applications in historic federal buildings. Hybrid work, mobile devices, and even austere environments all create new points of entry for attackers, but wireless technologies, when deployed with modern security frameworks, can help close gaps without introducing risk. "Our job is to take networks and extend them where they don't currently exist, so we can help our customers connect their people, places, and things very simply, securely, and easily for them to manage," DeVol said.

Safeguarding mission performance requires uniting physical infrastructure, wireless networks, and security frameworks into a single design. Secure systems must align with how employees actually work, ensuring a seamless user experiences that don't force trade-offs between productivity and production. As Copeland underscored, success depends on government and industry working together to integrate underlay networks with overlay specific to applications and offices to ensure that every layer of connectivity is inherently secure and resilient.

From problem to opportunity: leapfrogging the gap

Rather than trying to catch up incrementally, agencies have an opportunity to leap ahead by adopting wireless-first strategies, cloud-native architectures, and automation. "Look at this problem as a leapfrog effect," McFadden urged. "How do we help you get past the tech challenges and the debt you incurred?"



Technologies such as private 5G, Wi-Fi 6/7, and SD WAN (FedRAMP High) provide a foundation for modernization while reducing human error and enabling faster, more consistent deployments.

But as McFadden emphasized, technology alone isn't the point: "The end goal is to achieve the business outcome, which is driven by strategy and vision." Meeting that goal means designing systems around how people actually work, aligning investments to mission priorities, building capacity and cybersecurity from the start, and ensuring solutions support hybrid, mobile, and field-based operations.

Public-private partnership is essential

Modernizing infrastructure is more than a technology challenge; it impacts the entire ecosystem. No single agency or vendor can tackle this challenge alone. "Work with your industry partners," Copeland emphasized. "And let's work on outcome-based resolutions to any one of those problems."

Private sector partners like Verizon, Leidos, and Ericsson bring together diverse capabilities, including networks, security frameworks, management platforms, and field expertise, to create solutions that are more adaptable and resilient. As DeVoll noted, flexibility is critical: "Keep an open mind to how you provide connectivity and security because what worked five or six years ago isn't going to work in today's environment."

Building future-ready workplaces through partnership and innovation

The federal workforce is returning to offices with higher expectations and more complex needs than ever before. Meeting those needs requires a shift in both technology and mindset, prioritizing user experience, leveraging wireless solutions, and embracing a layered, secure approach to connectivity. By working together, agencies and industry can not only close the gap but leap ahead, creating resilient, future-ready environments that support mission success.

> **"We're not just here to sell technology," Copeland stressed."We're here to partner with the government to ensure that we are able to get the return-to-office experience to where it needs to be, now and into the future."**

carahsoft

Discover more about Carahsoft's 5G solutions
and our trusted partners.

carah.io/5Gsolve ☎ (888) 964-7379 ✉ 5G@carahsoft.com