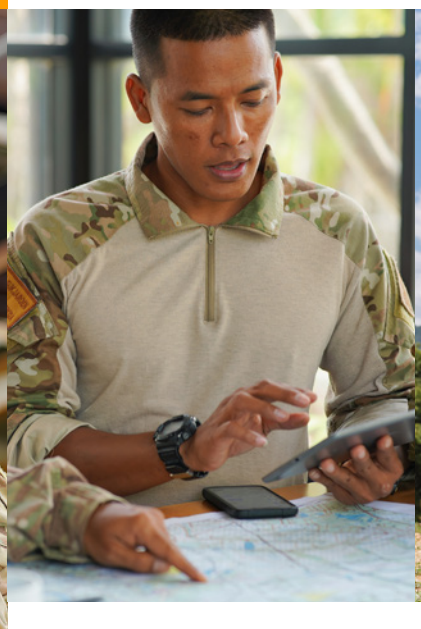

HPE aruba networking

4 priorities for agencies adopting 5G

The federal government is undergoing a digital transformation and when it comes to adopting 5G, the goal is clear: position the US as a leader in the next generation of technologies, ensuring reliable, secure and supportive private networks.

HPE GreenLake

Private 5G enhances government
Cybersecurity concerns and connectivity challenges are growing in the public sector, emphasizing the need for secure and seamless communication. A dedicated private 5G network is crucial for government operations as it can effectively support classified applications.

As the public sector aims to boost communication capabilities, it must address security concerns, ensure regulatory compliance, and embrace technological advancements for successful adoption. Additionally, collaborative efforts between the government and industry partners will be instrumental in shaping the future of secure and dependable private 5G networks. During a recent webcast with HPE Aruba Networking and GovExec, experts explored how private 5G is evolving and its role as the future of public sector communication.

1. Put security first

As the Department of Defense (DoD) incorporates 5G technology, security emerges as a top concern, especially in military applications. While 5G promises enhanced communication and connectivity, it also introduces new challenges and vulnerabilities that must be addressed to protect sensitive and classified information.

For example, one critical security concern involves implementing robust measures to safeguard data transmitted over private 5G networks. In dynamic and austere environments like military operations, where rapid deployment of new systems and low-latency communication is crucial, securing sensitive information takes precedence.

Thomas Rondeau, principal director of futureG & 5G for the Office of the Under Secretary of Defense for Research and Engineering, emphasizes the critical importance of security, particularly as 5G extends to tactical edges and potentially hostile environments. Rondeau categorizes security into three areas: ensuring the security of the technology supply chain, managing signals on networks and protecting against cyber threats.

Supply chain security involves scrutinizing the adoption of commercial off-the-shelf technologies to ensure the security of the supply chain. Operational security focuses on managing signatures in the radio spectrum and on networks, especially as the DoD leverages existing civilian commercial networks. Cybersecurity, the fundamental aspect of protecting systems from unauthorized access and manipulation, is highlighted as essential for maintaining military unit performance.

“5G standards have brought a lot more interest in security to the network than ever before, but it’s not quite enough,” Rondeau said. “These three categories together help us create additional layers of security and observability of what’s going on and the ability to quickly respond and react when advanced, persistent threat attacks occur.”

5G CFT is the nexus for deploying 5G and implementing it within the department, so we have a lot of good information and partnerships, not only with the military departments, but fromour other interagencies.

— **Juan Ramirez**, director of the 5G Cross-Functional Team for the Office of the DoD Chief Information Officer

2. Build strong partnerships

Successful 5G adoption lies in robust partnerships. According to Steve Lasko, a private cellular evangelist for U.S. Federal at HPE Aruba Networking, the qualities of a great partner include active listening, forward-thinking insights, effective communication, adaptability and understanding of budget constraints. For example, a valuable industry partner for the Department of Defense would be one that tailors solutions to meet the specific communication and connectivity needs of the DoD.

In support of this, Jonathan Ashdown, senior electronics engineer for the Information Directorate at the Air Force Research Laboratory, shared lessons learned from deploying 5G at Hill Air Force Base, underscoring the need for collaboration with industry partners. “Deploying 5G is one thing, but having an open 5G network where third party solutions can integrate with it is a whole other ballgame,” said Ashdown. “We learned that for DOD applications, 5G out of the box doesn’t give you exactly what you need commercially, but in working collaboratively with others, you can get it to where you need to be in a relatively short time scale.”

3. Consider the cost of a technological transition

Transitioning from traditional communication to private 5G involves a significant change, and maintaining a private 5G network poses its own set of challenges within budget limits. However, recent advancements in the private cellular industry bring promising solutions, and progress in smart logistics, low-latency communications and rapid deployment signifies a transformative era.

For government leaders embarking on the 5G journey, tapping into the resources and expertise of the 5G Cross-Functional Team (CFT) could prove invaluable. According to Juan Ramirez, director of the 5G Cross-Functional Team for the Office of the DoD Chief Information Officer, the CFT is a central hub for implementing and deploying 5G within the DoD, offering a wealth of information, partnerships and an acquisition playbook.

“5G CFT is the nexus for deploying 5G and implementing it within the department, so we have a lot of good information and partnerships, not only with the military departments, but fromour other interagencies,” Ramirez said. “We’re here to provide those lessons learned, but also ensure that you budget the sustainment because technology is always changing and you need to have that right path for technology enhancements.”

4. Strategize for compliance and integration

In federal operations, adhering to strict regulations becomes paramount when venturing into private 5G solutions. However, challenges arise when agencies look to integrate private 5G with existing communication systems.

One of the complexities involves securing the necessary frequency spectrum for private 5G networks, a process that demands intricate coordination with regulatory bodies. Scalability and interoperability also add another layer to the challenge.

In addressing these regulatory compliance and integration challenges, comprehensive strategies are essential. According to Ashdown, collaboration between government and industry partners is crucial to overcoming these hurdles. It's not just about following rules and fitting systems together; it's about building a strong foundation for the future of communications.

"When deploying 5G to enable warfighter success, the biggest focus should be on integrated comms systems for facilitating seamless interoperability between various military branches and coalition partners," said Ashdown. "Being able to share and leverage information across the services is of utmost importance to be able to be successful in the future and being able to share critical information efficiently amongst each other."

In a complex landscape of 5G adoption, meeting regulatory compliance and integration challenges requires a balance between adherence, innovation and collaboration. As the federal government embarks on this transformative journey, the goal is not just compliance but building a communications infrastructure that stands the test of time.

Learn more

Learn more about how HPE Aruba Networking is securing 5G for the public sector.

Visit **ArubaNetworks.com**

Make the right purchase decision.
Contact our presales specialists.

Contact us

Hewlett Packard Enterprise

SO_Federal-Agencies-Adopting-5G_RB_022324 a00137812enw