FEDERAL NEWS NETWORK

EXECUTIVE BRIEFING SERIES

DoD hones 5G requirements, priorities as rollout builds momentum

We build smarter future-ready bases, so you can focus on the mission.

Verizon's intelligent edge network unifies IT systems and IoT devices to drive our smart base solutions. They can help create more realistic training exercises and inform faster data-driven decisions, so your team is better equipped for the mission ahead.

Learn more at verizon.com/smartbase

verizon✓

DoD hones 5G requirements, priorities as rollout builds momentum

BY DAISY THORNTON

"Faster speed, lower latency." That's almost a mantra when people talk about 5G. Those two essential benefits will enable the innovations — think autonomous vehicles and augmented and virtual reality — that drive the hype.

But the Department of Defense (DoD), which has been experimenting with 5G for years at bases across the country, intends to move past the hype and get serious about 5G use cases and mission-critical capabilities.

"5G, in and of itself, is not a requirement. It's a solution to a requirement. It's getting out there and defining what are the real mission requirements, so we understand where 5G should be prioritized and how it should be implemented," said Rob Beutel, deputy chief technology officer for the Air Force. "Because 5G is so much more than my phone having faster speed. It is ... edge computing. It's the tremendous density to improve Internet of Things and sensor devices out there. It's all those things. It's really less about the consumer and more about the mission itself and the great capability that it brings to us."

On that front, DoD's private sector partners are in lockstep with the department. In January, Verizon completed its first acquisition of C-band spectrum, which will allow it to deliver the broadband needed to lay the foundation for use cases more widely across the DoD enterprise.

"One of the big use cases that we've seen, not only in the DoD but across the federal government, is actually just raw broadband services. We look at 5G as offering that type of service to close the digital divide in a lot of cases," said Bryan Schromsky, managing partner of 5G Public Sector at Verizon. "We're talking anywhere from recruiting offices to providing broadband in remote

> " It's very exciting to talk about the bits and the bytes ... but more importantly, what is the application or the problem or business outcome we're trying to achieve that 5G can enable?
>
> — Bryan Schromsky, Managing Partner of 5G Public Sector, Verizon

areas and rural communities. It's huge. And having one network infrastructure to support all these different technologies is very exciting."

DoD wants that infrastructure to be interoperable. Beutel said that the Air Force decided to use the reconstruction of Tyndall Air Force Base in Panama City, Florida, as an opportunity to be more forward-thinking about its IT. As part of Tyndall's Installation of the Future program, the service wants to develop a multivendor implementation that will be the model for DoD installations moving forward.

The Air Force isn't operating alone or on a hunch. Multivendor implementation for 5G networks is a priority across DoD. In April, the department

launched a 5G innovation competition to accelerate the "development and adoption of open interfaces, interoperable components and multivendor solutions toward the development of an open 5G ecosystem," DoD noted in its announcement about the competition.

The goal of the challenge is to create a large vendor community that will help DoD build a plug-and-play environment with 5G. Much of the current ecosystem uses custom software and hardware that often increases costs and leads to security issues, said Daniel Massey, program lead for the 5G Initiative at DoD. The department needs to be able to create data-centric weapons systems that can communicate with one another, he added.

Viewing 5G as critical infrastructure

For Massey, the biggest mission requirement is the ability to operate through commercial infrastructure anywhere in the world. Ultimately, 5G is like any other critical infrastructure. If DoD is operating overseas, it doesn't build its own bridges, roads and airfields if it doesn't have to, he said. It has the capability and resources to do so if necessary, but it only commits resources when it must. Communications, Massey contends, should be the same.

That's not to say DoD isn't interested in private networks. Sometimes Defense organizations or the services must deploy their own infrastructure. To that end, the U.S. Army Corps of Engineers has been building such a capability, said Chief Information Officer Dovarius Peoples. USACE has rolled out 5G to 44 of its 50 sites so far and is working on the ability to rapidly deploy it in disaster relief situations too. The idea? To be able to restore telecommunications to an affected area, Peoples said.

But typically it doesn't make sense for DoD to try to compete by building its own bespoke, proprietary infrastructure, Beutel said.

DoD technology leaders realize that some of its needs are not special or unique to the department. Numerous applications were once solely within DoD's purview, but now the private sector has advanced some of these capabilities, Beutel said. As an example,

> ## "
> ### 5G, in and of itself, is not a requirement. It's a solution to a requirement.
>
> ### — Rob Beutel, Deputy Chief Technology Officer, Air Force

he pointed to Starlink's role in aiding Ukraine in the conflict with Russia.

"Look at how Starlink was able to get capability in place very quickly and then mitigate issues very quickly. That's not something you can typically do when it's a DoD-owned capability. We're not nearly as agile," he said.

The private sector has invested trillions of dollars in 5G. DoD wants to reap the benefits of those investments instead of competing with them, Massey said.

"We would like to go in and, when appropriate, leverage existing commercial infrastructure — just like we would leverage existing roads and bridges when appropriate — and also, when appropriate, be able to bring our own infrastructure," he said, calling the commercial infrastructure "fantastic" because of the investments and improvements made by organizations across the technology industry.

The main concerns involve security, Massey said. "Can we make that infrastructure secure enough for various DoD missions? I think that's one of the interesting open questions."

Understanding 5G security

There are four aspects to the question of security: confidentiality, integrity, availability and observability. The first three are classic security considerations. Is

secret data being protected? Is it unmodified? Is it accessible for use by those who need access to it?

But observability, previously considered to be an element of the first three, is growing in importance. Sometimes, even if data is encrypted so that it can't be viewed or modified, knowing minimal information — such as the parties communicating with one another — can let observers infer a good deal of information. DoD isn't working on this problem alone.

In May 2022, the department's Research and Engineering Division, in collaboration with the Cybersecurity and Infrastructure Security Agency and the Homeland Security Department's Science and Technology Division, released a new 5G Security Evaluation.

The evaluation lays out a five-step process for assessing a 5G system and identifying potential security requirements necessary to move it into production. The process builds on earlier assessments, like the National Institute of Standards and Technology's Risk Management Framework.

Prioritizing 5G rollout across DoD

For DoD as a whole, a top priority is the rollout of a 5G radio access network, particularly the agility of the spectrum and the ability to share it, Massey said. At the physical layer, that means transmitting bits across the air. There's lots of contention for space

> ## "
> ## We would like to go in and, when appropriate, leverage existing commercial infrastructure — just like we would leverage existing roads and bridges when appropriate — and also, when appropriate, be able to bring our own infrastructure.
>
> ## — Daniel Massey, Program Lead for the 5G Initiative, Defense Department

and the spectrum itself. DoD is working on how to appropriately use and share that spectrum, he said.

That's one reason Verizon is focusing on building out its network, including its new C-band, as well as new spectrum licenses being rolled out by the Federal Communications Commission. Verizon has seen demand for mid-band radio spectrum, including millimeter wave frequencies, across the federal government, Schromsky said.

For example, the Defense Logistics Agency and USACE are using it for new smart warehouses. The Veterans Affairs Department's surgical centers are using it for 3D imaging. And VA's medical campuses plan to use a variety of spectrum to cover different uses, including millimeter wave and mid-band for outdoor connectivity, and even 4G for monitoring medical device data.

"Building out infrastructure is probably the biggest thing going on for us right now," Schromsky said. "Because as you can imagine, we have many use cases. It's not just the devices themselves. But there's a huge broadband initiative that we see in 5G, what we call fixed wireless access."

What's more, 5G supports lots of wired connectivity as well, not just wireless and mobile. That's not cheap to install, Peoples said.

"We're also beginning to look at our backend infrastructure and networks, because with 5G, there's a significant amount of fiber that needs to be laid as well in order for that to be successful," he said. "And when it comes to laying fiber, that also requires a significant financial responsibility. So the funds are something that we're definitely looking to enhance. Granted, within the government, you have to be very strategic when it comes to future planning."

That focus on the backend infrastructure and wired connectivity will enable other use cases for 5G, Massey added. It will make a 5G core network possible, along with the various capabilities that would entail, like network slicing. Slicing, the ability to layer essentially a virtual network on top of the existing network, would provide DoD with added security and performance.

Finally, DoD is looking to 5G to prioritize edge computing capabilities, Massey said. The department's many and diverse organizations often operate in environments where connectivity back to a central cloud is unreliable at best, he noted. Pushing compute out to the edge will give components in the field more ability to analyze data to inform decision-making.

That's something that Peoples said is very important to USACE as it continues transitioning to a fully hybrid work environment. Before the pandemic, 70% of USACE operated remotely. That's up to 90% now, and Peoples doesn't expect that to change anytime soon.

"I see the enablement and the use of 5G technology to enhance the end-user experience. What does that mean? We have construction engineers and many different, not just construction, sites. We have engineers at levees, locks, dams and those type of things," he said. "So being able to work optimally, in

"

I see the enablement and the use of 5G technology to enhance the end-user experience … so being able to work optimally, in a less controlled environment, but more so in a free space as an engineer.

— Dovarius Peoples, Chief Information Officer, U.S. Army Corps of Engineers

a less controlled environment, but more so in a free space as an engineer, that's improving the user experience."

5G will let remote users access not just data but other mission-critical elements and also share information with external partners, People said.

But, Massey reiterated, all these priorities are heavily dependent on security. Without proper security, DoD can't share spectrum safely, slice core networks or realize the full potential of edge computing, he said. That's where the federal government's massive push to adopt zero trust architecture comes in. In a 5G, hybrid world, there is no more castle and moat, no more inside and outside the network, Massey said.

Communicating needs to the private sector

As adoption of 5G takes place, it's going to be important for federal agencies to learn how to effectively communicate evolving needs to industry partners, Beutel said. That's the only way DoD will be able to prioritize the right 5G solutions on smaller scales, he advised.

"We need to really, really … define our requirements, understand the use cases, what we're trying to do, so we're applying the right capability to the right situation," Beutel said. "So many of the cases, we have people in the field coming back saying, 'I need 5G.' That's not the requirement. We need you to come to us and tell us what it is you need to do. Because it's really hard to defend that in the budget, and it's hard for our vendors out there to understand."

Schromsky agreed. As 5G capabilities roll out over the near future, "it's very exciting to talk about the bits and the bytes … but more importantly, what is the application or the problem or business outcome we're trying to achieve that 5G can enable?" That must be first and foremost, he said.

The sources in this article shared their comments during a Federal Executive Forum, presented by Trezza Media Group.

Want to try out that device on 5G? Take it to a lab

Both inside the government and in industry, testing facilities make it possible to run a device in a real-world-like space without compromising an agency's actual networks.

Both the U.S. Army of Engineers and Verizon have launched facilities that can do that.

USACE created a Cybersecurity Center of Excellence focused on operational technology. The center's team can assess 5G technologies, as well as other functional capabilities like zero trust, from an operational perspective, said Dovarius Peoples, the corps' chief information officer. Though that often isn't discussed in depth, it's critically important once a technology moves into a live production environment, he said.

"Within this Cybersecurity Center of Excellence, from an operational technology perspective, these are the same technical capabilities that will allow us to secure as well as operate efficiently when managing and maintaining things such as levees, locks, dams, many different infrastructure, critical waterways and those type of things," he said. "That Cyber Center of Excellence has really allowed us to be able to look at full-spectrum operations and many other things. And it's also allowed us to be able to assess operational technology through the leveraging of 5G technical capabilities. And we've seen a lot of success as well as challenges."

Meanwhile, Verizon launched a lab in downtown Boston that mimics the vast majority of what Verizon's 5G network does today, said Bryan Schromsky, the company's managing partner for 5G public sector.

Agencies can come in and test things, like Verizon's new quantum key distribution network, without having any potentially adverse effects on the commercial network, he said.

"Having the ability to do that in a confined space is very exciting. A lot of agencies are very interested so they can get raw data on how a device interacts with the network," Schromsky said.

The focus on data and learning how devices perform on 5G networks won't be confined to the new lab only. Verizon also will begin experimenting with autonomous vehicles and drones at Marine Corps Air Station Miramar later this year. A goal will be to determine what data can be extrapolated.

That's also a consideration with Internet of Things devices, Schromsky said. He foresees millions, if not billions, of IoT devices eventually being implanted in nonelectrical tools, even uniforms and boots.

Those types of devices won't use much bandwidth compared to others, like augmented reality eyewear and virtual reality headsets, that require low latency and high bandwidth. Depending on the implementation, some IoT devices might leverage 4G networks to report out and share data, he suggested. Even so, those uses would still be part of the broader 5G ecosystem, just on narrower bands or even wireless broadband.