

EXPERT EDITION

Preparing for federal networks of the future

Insights from

- DoD
- DISA
- Navy
- NTIA

BROUGHT TO YOU BY **carahsoft**

Transforming Government Networks with **5G Wireless** Solutions

For more information, visit
carah.io/5Gsolve



CONTENTS

Are you ready for 5G and more?	3
DISA's PEO Transport wants 'graceful transition plan' for network convergence	4
How end-to-end private networks offer connectivity, comms on prem and at the edge	7
Navy project brings promise of cloud, network access anywhere to the middle of the ocean	10
How private 5G networks can help agencies address operational complexity, security and connectivity	13
DoD rolls out free Wi-Fi to barracks	16
How private 5G networks are unlocking information, communication dominance on the battlefield	18
Q&A with the National Telecommunications and Information Administration's Evan Feinman	21
How private 5G networks make AI at the edge practical, secure	26



FEDERAL NEWS NETWORK

Ask the CIO

with Jason Miller

Listen. Read. Engage.

[Click to Listen Now](#)

A **Federal News Network** Podcast





Are you ready for 5G and more?

As agencies continue to push toward anywhere access to network services and data, a critical piece continues to be modernization and a move away from legacy and government-owned network backbones.

In the pages ahead, we look at some of these federal efforts and also share insights about the evolution of 5G capabilities and how they are changing what's possible as the government modernizes and adopts transport-agnostic network services.

For the larger agencies, maintaining services while modernizing is a critical challenge, especially when working to collapse and unify disparate networks.

As Maj. Gen. Christopher Eubank, commander of the Army Network Enterprise Technology Command, shared with [Federal News Network in early 2024](#) — as the Army had gotten down to 14 networks on its way to one: “What we don’t want to do is to converge ... and then figure out we’ve broken a bunch of stuff.”

But the need for cost-effective network infrastructures that support mission needs continues to drive agencies forward.

Points out Bob Stephenson, chief information officer for U.S. Pacific Fleet: “We’ve been using the same technology in our buildings that we’ve used since the late ‘90s. As our staff changes and grows, it’s very difficult for us with a wired infrastructure to bring more people into the building or rearrange the office. We’re doing a pilot ... where we’ve gone to wireless in the buildings.” (*Read more now on Page 10.*)

The blending of 4G and 5G solutions creates the potential for agencies to improve the ability to support employees whether at a federal office or at a remote or in-transit location. “The federal government needs networks that can really keep up with the evolving needs and be able to provide reliable and secure connectivity no matter where their employees are located,” explains Mike DeVol, Ericsson’s federal area vice president. (*Read more now on Page 13.*)

In addition to the Navy and Ericsson, the articles in our e-book feature experts at the Commerce and Defense departments, Defense Information Systems Agency, Druid Software, HPE and Intel.

We hope the e-book provides your agency helpful tips and tactics on preparing its own network services for the future.

Vanessa Roberts
Editor, Custom Content
Federal News Network

DISA's PEO Transport wants 'graceful transition plan' for network convergence

BY ANASTASIA OBIS

The Defense Information Systems Agency's Program Executive Office for Transport provides the foundational infrastructure for the Defense Department's networking — it oversees satellite communication gateways, integrates command and control systems and operates the transport for internet access points.

The office works closely with [DISA's J9 hosting and compute directorate](#) to ensure

that the cloud access providers have the necessary network infrastructure to support reliable communication and data transport. It also helps the J6 endpoint services and global service center make sure that various locations are interconnected and can communicate seamlessly.

"We are like the electric company. No one knows about us until something goes wrong — the same thing goes with the Transport," Chris Paczkowski, director of PEO Transport, told Federal News Network.

Paczkowski's office is essentially the internet for the department. This means that the office oversees a wide range of network and communications programs, each with its own goals and objectives, making it challenging for Paczkowski's teams to manage those projects in a more integrated way.

Keeping a focus on standardization, cost

Paczkowski said the office is looking to standardize to create consistency across more than 50 projects the office manages. It is also moving toward more centralized contracts, particularly in areas such as cybersecurity. And

We're hoarders. If there is something that works — I'm going to use this until it doesn't work anymore because I usually don't have the dollars to keep trying to do the next greatest thing.



Chris Paczkowski,
Director, Program Executive
Office for Transport, DISA

as the Defense Department is moving toward adopting next-generation networking gear, PEO Transport is seeking standards-based solutions from multiple vendors.

But DISA is dealing with a mountain of legacy equipment as new technology gets piled on, he pointed out.


"We're hoarders. If there is something that works — I'm going to use this until it doesn't work anymore because I usually don't have the dollars to keep trying to do the next greatest thing," Paczkowski said.

Making changes on the go

That's why DISA looks for new technology capabilities with what he called lifespan standards. "We have thousands of pieces of equipment. And just imagine if all the highways getting into Baltimore were going to get paved today and so they shut it down just to do the paving," Paczkowski said.

"That's no different than when we have to say, 'Hey, we have to upgrade our equipment. Let's take down this link to be able to do that.' And the response is, 'No, I've got a conference, I work at the hospital, fire department, I need to be going to work.' Trying to balance that is another reason why we have to find a capability that has that longevity and flexibility for us to be able to implement things in a parallel manner."

To address the issue of mounting legacy equipment, Paczkowski said he wants to see more roadmaps and more "graceful transitions" from industry.



We have to find a capability that has that longevity and flexibility for us to be able to implement things in a parallel manner.

— DISA's Chris Paczkowski

"Everyone wants to sell something new and, and when this is done, then I get something else that's newer. There isn't really a graceful transition plan in those cases if it's nonstandards-based," he said.

In addition, Paczkowski said the components need to prioritize infrastructure upgrades even despite budget constraints,

"If you have an iPhone 7 — no one does anymore — but we have a lot of iPhone 7s. We're hoarders in the department. Well, now my app doesn't really work, now we need to upgrade. Well, I don't have money for a phone. Well, if that's a priority, make sure that you need to be keeping up with your infrastructure. Because not just from a functionality perspective, with the legacy challenges their cyber components to it, there are vendors saying, 'Hey, I'm not supporting that anymore.' So again, it is prioritization." 🚧



INNOVATION IN GOVERNMENT

Be part of a more responsive and secure government by learning from experts about how to enable innovation.

**TUNE IN EVERY TUESDAY AT 10:30 AM & 2:30 PM ET
FOR THE FEDERAL NEWS NETWORK SHOW**

- Listen to podcasts
- Read success stories
- Watch interviews and panels

Sponsored by **carahsoft.**

How end-to-end private networks offer connectivity, comms on prem and at the edge

One of the first priorities for Federal Emergency Management Agency employees responding to a disaster zone is to set up a communications infrastructure. The same is true for warfighters in a remote, hostile environment.

Those are two very different kinds of federal employees with two very different missions. Even so, one thing ties them together: Without communications, they can't coordinate, leaving them less effective.

The common picture of a federal employee is of someone behind a desk in a Washington, D.C., headquarters building creating policy. But the truth is that federal employees perform myriad different missions in every environment imaginable, all over the world — and in a handful of cases, beyond it — and the ability to communicate is critical to all of them.

When these employees are operating in the field, beyond the reach of regular communications infrastructure — or when that infrastructure has been denied to them for one reason or another — they have to be able to provide their own. Complete 4G/5G systems can run at the edge, allowing a variety of endpoints to connect to the back-end system,

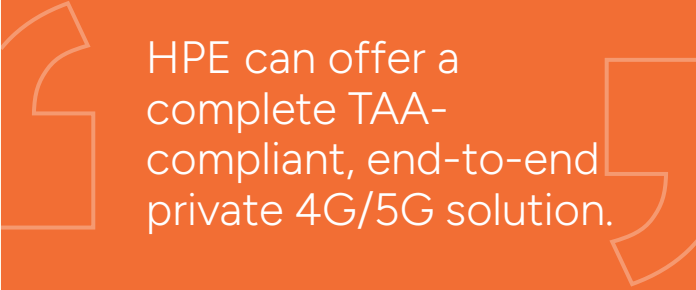
in sizes ranging from a tower on a building, down to a portable system used for disaster recovery.

"In such cases, we just provide a carriable server or a small backpack with a battery, and also with Starlink or satellite communication," said Venkata Sunil Prasad Meda, solution architect at [HPE](#). "We will be able to connect or provide connectivity at that area, with close to 1- to

A fast, deployable portable kit ... can be made available at the edge, and it can be brought up in five to 10 minutes when you turn it on. And the devices that are connected to it will have immediate connectivity.



Venkata Sunil Prasad Meda,
Solution Architect, HPE



HPE can offer a complete TAA-compliant, end-to-end private 4G/5G solution.

— HPE's Venkata Sunil Prasad Meda

2-kilometer range. So you can imagine a fast, deployable portable kit that can be made available at the edge, and it can be brought up in five to 10 minutes when you turn it on. And the devices that are connected to it will have immediate connectivity.”

Another use case Meda said HPE is working on is flight line connectivity. Traditional Wi-Fi struggles on flight lines, making connectivity difficult. But when a plane lands, there’s a significant amount of sensor data that needs to be immediately downloaded. A single cell tower can provide connection on the entire flight line, enabling the data to be downloaded through cellular connectivity.

Federated and hierarchical features

Another advantage of these complete 4G/5G systems is their ability to be federated. Private systems often don’t talk to one another because they’re competing for the same signal. Meda likened it to a pair of fire trucks with the same equipment.

“A fire truck equipped with a private 4G/5G solution will have its own set of devices to do the mission critical activities like push-to-talk, video calling, et cetera. Comms are good as long as a fire truck is nearby providing radio signal and backhaul,” he said.

“If it’s a big accident and one or more fire trucks come in, there are chances for the devices — as they use the same radio frequency signal — to bounce back between the fire trucks. And it’ll be causing some discontinuity on the device phone signal because now two or more trucks are providing the same frequency radio signal.”

HPE solves that issue with its patented federation system. If two or more core 4G/5G systems come into proximity, they automatically form a cluster. The device traffic will automatically route through one 4G/5G core. That maintains continuity of communications and allows multiple teams to coordinate and break apart seamlessly as needed. Meda said this can be a game changer in disaster recovery or combat scenarios.

There are also hierarchical setups, where multiple private networks can be subordinated to a single command and control center with a hierarchical dashboard. That allows a single centralized point to manage multiple distributed clusters across a large geographic area, such as environmental disaster areas and U.S. military bases overseas.



Modernize, Secure, and Scale With HPE Aruba Networking

HPE Aruba Networking's security-first, AI-powered approach enables federal agencies to transform their operations and expedite mission response with scalable, secure, and agile networking solutions

[Learn more](#)

 **Hewlett Packard
Enterprise**



From the central control center, network teams can provision or retract new devices and push out policies in a uniform manner. But each network is also private and individual. If the central control center is cut off, the individual networks will continue to operate until connection is reestablished, at which point they automatically update to stay in compliance.

"HPE can offer everything end to end," Meda said. "We can offer the 4G/5G software, including voice services, and add a federation

module if required. On top of it, we'll can offer the complete package on HPE hardware. Plus, we can provide the all-in-one radio access network. We partner with various device manufacturers or gateway-providing companies so that, if required, we can provide the gateways to the government. So HPE can offer a complete TAA-compliant, end-to-end private 4G/5G solution." 🚀

Navy project brings promise of cloud, network access anywhere to the middle of the ocean

BY JARED SERBU

From [virtual desktops](#) to email and collaboration, the Navy has been [leaning heavily on cloud services](#) to speed up its digital modernization efforts. But those efforts have come with a big question: Will any of this work aboard ships? It turns out the answer is yes.

In a pilot project, the Navy has shown it's possible to consistently move several terabytes of data each day between the cloud and thousands of users onboard an aircraft carrier every single day, an advance officials say is a game changer.

The project is called Flank Speed Edge, an extension of Flank Speed, the Navy's broader cloud environment. The largest test case has been aboard the USS Abraham Lincoln, which had been underway in the Pacific throughout 2024, and represents the first major example of the Navy providing network connectivity for a vessel at sea with cloud services in a way that's on par with what sailors get on shore.

Leveraging P-LEO satellites

It's mostly thanks to the [advent of proliferated low-Earth orbit \(PLEO\)](#) satellite services — massive constellations of small satellites that form mesh networks via optical links with one another in space and deliver high-bandwidth, low latency communications to users back on Earth.

Cmdr. Kevin White, combat systems officer aboard the Lincoln, said the initial idea was to install a gigabit's worth of satellite connectivity aboard the ship and see what the ship's 5,000 sailors and Marines could do with it. It turns out, quite a lot.

"I've seen a tremendous value from this afloat. All of the staff are using their Flank Speed capabilities to maintain continuity," he said during a live video demonstration from the Pacific Ocean for a Navy CIO Office conference. "They're using their NMCI phones to call home over voice over IP, or to call the beach to say, 'Hey, I need this part rushed to the ship.'"

"We're using it across all of our departments and embarked commands for quality-of-work type areas. Everything from our training department — ensuring that all of our readiness in our training cycle is up to date — to our medical department, to our supply department. They're all reaching out over websites and services to ensure that we have continuity of operations and ensure that this ship is ready to go when the time comes that we have to turn these services off."

One thing the Navy has learned from the Lincoln experience is that Flank Speed Edge doesn't require a huge workforce. It's taken just three

full-time sailors to operate and maintain the new satellite and Wi-Fi infrastructure aboard the carrier.

And in return, it's also dramatically expanded the kinds of software upgrades and updates that can be performed on other systems on the ship, White said. Traditionally, that's the kind of work that can only be done at a pier with a physical network connection.

"While we're out at sea right now, with this PLEO capability, a cloud-connected node and all the right elements in place, we're able to scale new capabilities as they become available and rapidly deploy them while they're monitored from the shore side," he said.

"One of the big challenges we have is the cycle of Windows updates and the cycle of patches. With that high-speed capability, we can have those update services enabled. Onboard, we have 2,000 staff folks, all of which are live at their home commands on Flank Speed. Imagine a future where we are able to migrate that data to an embarkable [laptop] and allow them to interoperate with that data when we have to turn off our connections."

Working through comm challenges

The approach does have its limitations. Besides the obvious need to sometimes shut down those high-speed data links for operational reasons — leaving the ship with only its onboard tactical cloud nodes — the PLEO connections, so far, are only authorized for unclassified data.

But White said the onboard infrastructure is designed to be transport agnostic — so that it

Flank Speed is a vast improvement compared to the previous assets and legacy architecture. The user interface is quick and responsive. Applications are able to be opened natively instead of using browser-based workarounds. Simple things matter here: The file sync is seamless.



Lt. Cmdr. Tricia Nguyen,
Staff Member, Naval Computer
and Telecommunications
Station Bahrain

can use whatever connectivity mechanism is available — from traditional military SATCOM to commercial services like Starlink. It's also designed to incorporate software-defined networking, so that the network capacity available through those data links can be used however the Navy sees fit and can be reallocated on the fly.

"Right now, our logs are showing that we're able to pass between 3 and 5 terabytes of data per day, which is absolutely massive. And what we're able to do with software-defined networks is scale exactly how that data is used," he said. "Right now, we're demonstrating pushing applications like air wing maintenance apps that

live in the cloud and all of our pay and personnel apps. And that's just scratching the surface."

Using applications ashore

The Navy is using similar concepts in other places of the world that may not be as hard to connect as ships but still have tended to have communications challenges.

The service's 5th Fleet is serving as a pilot site for a shore-based implementation of Flank Speed Edge. At the command's headquarters in Bahrain, staff have recently started using Flank Speed services, including Nautilus Virtual Desktop.

Lt. Cmdr. Tricia Nguyen, staff member at Naval Computer and Telecommunications Station Bahrain, said so far the Flank Speed approach has turned out to be more seamless and resilient than the Navy's traditional overseas networks.


"It is a vast improvement compared to the previous assets and legacy architecture," she said. "The user interface is quick and responsive. Applications are able to be opened natively instead of using browser-based workarounds. Simple things matter here: The file sync is seamless. I don't have to log in multiple times like I used to. Now, I just boot up and my files are there. And back in March [2024], there was a Teams service outage, which I understand was worldwide. However, here in Bahrain, we did not experience an outage at all. That was because of the architecture: We have a primary and secondary means of transport that are terrestrial-based and a tertiary that's commercial satellite. We had an automatic failover, and it was completely seamless and transparent to our end users. I didn't even know about it until after the fact."

We've been using the same technology in our buildings that we've used since the late '90s. ... We're doing a pilot sponsored by PEO Digital where we've gone to wireless in the buildings. ... This is going to give us an enormous capability to modernize our buildings like we're modernizing our ships.



Bob Stephenson, CIO,
U.S. Pacific Fleet

Bob Stephenson, chief information officer for the U.S. Pacific Fleet, said some of what the Navy has learned through the pilots — especially their uses of secure Wi-Fi — may also be applicable to communications on installations, such as his command's headquarters at Pearl Harbor.

"We've been using the same technology in our buildings that we've used since the late '90s. As our staff changes and grows, it's very difficult for us with a wired infrastructure to bring more people into the building or rearrange the office," he said. "We're doing a pilot now sponsored by PEO Digital where we've gone to wireless in the buildings. We still have to use fiber for our secret networks, and we'd like to change that, but this is going to give us an enormous capability to modernize our buildings like we're modernizing our ships." 

How private 5G networks can help agencies address operational complexity, security and connectivity

Roughly half of the people who read this article will do so on a cell phone. That's because over the last couple of decades, cellular technology has integrated itself deeply into our day-to-day lives, changing the way we not only communicate but also travel, shop, read and even work.

Yet for all that, in the public sector enterprise space, cellular technology still lacks maturity. But that may be about to change, as networking

convergence toward private 5G network solutions offers ways to overcome some of the toughest technological challenges that federal agencies face.

"Operational complexity and the rise of these distributed workforces, they're changing the way we do things from a traditional networking standpoint," said Mark DeVol, federal area vice president for [Ericsson Enterprise Wireless Solutions](#). "The federal government needs networks that can really keep up with the evolving needs and be able to provide reliable and secure connectivity no matter where their employees are located."

Part of this is due to the proliferation of endpoint devices in the field; the pandemic sparked a sudden surge in devices outside the traditional network boundaries, but that proliferation hasn't slowed. That's triggered new challenges in the areas of cybersecurity and network management, as all of those endpoints are potential vulnerabilities.

Simplifying security solutions

That's one area where private 5G networks can help agencies. DeVol said these private 5G networks come with zero trust architecture as

The federal government needs networks that can really keep up with the evolving needs and be able to provide reliable and secure connectivity no matter where their employees are located.



Mark DeVol, Federal Area Vice President, Ericsson Enterprise Wireless Solutions

the default, simplifying what is otherwise a very complex solution. They can be set up with a very specific set of policies and controls, then deploy at scale and push those policies out to thousands of endpoint devices at the same time, saving network administrators significant time and effort. From that point on, devices without those particular authorizations won't be able to access the network.

"We just do things a little differently because we're using cellular as the primary wide-area network," DeVol said. "We're trying to help reduce the attack surface: hiding traffic, IP addresses, WAN resources from any kind of discovery by somebody who isn't authenticated or authorized onto the network. We also are trying to prevent any lateral movement by denying all by


default so nobody can connect until you have been pushed the policy to enable access and then provide user to resource access."

One of the benefits here is that's how cellular networks work already. When a device connects to a cellular 4G network, it's authorized by the Home Subscriber Service (HSS), a central repository of data regarding authorized users and device profiles on a network. The HSS authenticates the device, and routes it to the resources it has access to, like internet or a private network. This kind of device segmentation also means that applications are only available to devices that are authorized to access them.

Improving application availability

That said, many federal agencies have another challenge regarding application availability: making them available on a consistent basis wherever they're needed. For example, traditional Wi-Fi access points limit connectivity to about 300 feet line of sight. But depending on the type of cellular network an agency deploys, that connectivity could extend to half a mile. That means far fewer access points are necessary to provide total coverage to a facility like a million-square-foot warehouse owned by the General Services Administration.

DeVol detailed another potential use case for improving application availability for the Air Force.



By providing a private cellular network, we're trying to take the best of Wi-Fi and the best of cellular and bring it together, so we have a more robust yet simpler solution that can be deployed at much larger scale.

— Ericsson's Mark DeVol

"Flight line connectivity for Air Force maintainers and crew members is typically nonexistent because often the carriers don't have cellular coverage in some of those areas. All the flight crews or the aircraft maintainers have is Wi-Fi back in a hangar or office," he said. "So we are currently working with one Air Force unit and with a demo where we deployed a private cellular network on the flight line. And what this now allows them to do is connect their ruggedized laptops or tablets to be able to download their job orders for the day or blueprints or schematics for the aircraft that they're working on. They can now do all that at the aircraft site, whereas before they would have to go into the hangar."

DeVol said one of the main challenges for private enterprise 5G networks in the public sector is that lack of maturity translates to a lack of awareness and education. Federal technology executives largely aren't aware of what it can accomplish for them. That's why the first step in implementing one of these networks is finding a private sector partner and talking through what problems agencies are trying to solve and talking through the potential advantages.

"By providing a private cellular network, we're trying to take the best of Wi-Fi and the best of cellular and bring it together, so we have a more robust yet simpler solution that can be deployed at much larger scale." 🚀

ERICSSON 



High Performing, resilient and secure connectivity for government

[Learn More](#)

DoD rolls out free Wi-Fi to barracks

BY ANASTASIA OBIS

After former Defense Secretary Lloyd Austin rolled out a set of [“Taking Care of Our People” initiatives](#) in September 2024, the Pentagon’s has focused on ensuring service members have free and reliable Wi-Fi in remote barracks.

“Some of our barracks are very well set up to be able to just very easily plug in a router. One of the things that we’re doing is focusing on remote and austere locations where access is more challenging. Whether that’s a physical transformation of the building or whether it’s some type of retrofit — all of those are things

that we’re going to have to get after to be able to provide these services,” Brendan Owens, former assistant secretary for Defense for energy, installations and environment, said in late 2024.

Over the last several years, Defense Department officials have gathered feedback from junior enlisted personnel and military families to get a clearer picture of the challenges of military life. The feedback shaped a set of initiatives that Defense unveiled in the fall.

Moving toward a Wi-Fi-connected force

To provide and expand access to Wi-Fi, the Office of the Secretary directed all military services to create Wi-Fi pilot projects at no cost to service members, which will “form the basis of a long-term plan to build a Wi-Fi-connected force,” the OSD memo reads.

Owens said the need for internet access is more than just entertainment. Junior enlisted service members need internet access for mental health services, especially in places where behavioral health care access is limited and other resources, whether its online training, military and family life counselors, or simply connecting with family and friends.

This is certainly something that’s supported down in other parts of the building — that it’s a mission essential requirement.



Brendan Owens, Former Assistant Secretary for Energy, Installations And Environment, DoD

"This is certainly something that's supported down in other parts of the building — that it's a mission essential requirement," Owens said.

But DoD had to jump through a lot of legal hoops to first designate Wi-Fi as a mission critical service.

"That was a fair amount of groundwork that we had to do to overcome the legal barriers. We've got a bunch of legal precedent that we're working our way through," Owens said.

"After that, the challenge becomes, how does DoD partner with the installation and the service providers in those areas to make it possible for us to do that."

Planning still needed for DoD-wide barracks plan

Junior enlisted service members have long emphasized the need for having reliable, high-speed internet access.

"Every time we go and we visit barracks, one of the questions that I ask our soldiers, our Airmen, our Marines, our Guardians in those barracks is, 'If you could have 10 more square feet in your barracks room or free Wi-Fi, what would it be?' And no one is going to be surprised that a 19-year-old wants free Wi-Fi," Owens said.

While some of the services have already launched their own efforts to bring free Wi-Fi to military installations — the Department of the Navy launched a pilot program earlier this year to provide internet access to sailors living



The challenge becomes, how does DoD partner with the installation and the service providers in those areas to make it possible.

— *Brendan Owens*

in Virginia — it's not clear whether sailors will eventually get internet connectivity on ships during long deployments.

Internet connectivity on ships is often limited primarily due to cybersecurity concerns and bandwidth prioritization, the limited bandwidth is usually reserved for critical military operations.

In his memo, Austin directed the undersecretary of defense for acquisition and sustainment to work with the services to track Wi-Fi pilot programs and share best practices. Owens said the next step will be creating a departmentwide policy plan. 🚧

How private 5G networks are unlocking information, communication dominance on the battlefield

The Defense Department has long recognized access to information and communications as a key component of battlefield dominance. The advent of artificial intelligence, machine learning and other edge technologies has evolved those efforts, with the potential of putting more information at the fingertips of warfighters and allowing them to make informative decisions, faster. In a series of recent research projects, DoD has identified 5G as the primary enabler of those technologies and is actively driving initiatives to bring them to implementation.

Those research projects are now moving into production environments, with multiple authorities to operate for private 5G networks expected soon. As this shift occurs, private 5G networks will enable DoD to fully leverage capabilities like drones, augmented and virtual reality (AR/VR), autonomous vehicles, surveillance, smart logistics and much more.

DoD leaders are well aware of role that 5G can play in supporting mission.

Battaglia pointed to DoD's [Private 5G Deployment Strategy](#), which calls for accelerating the adoption of 5G technology to contribute to the warfighting capacity and lethality of the joint force.

"We must leverage emerging advanced technologies to become more efficient, effective, automated, and resilient. This includes a global, interconnected communications network that is robust, high performing, secure,

One major benefit of 5G is that it can be deployed using commercial servers in any one of a large emerging ecosystem of radio access network, or RAN, providers — all with easy-to-use management tools.



Paul Battaglia, Vice President of Public Sector, Druid Software

agile and robust — designed to accommodate scalability, rapid adaptation for war and rapid reconstitution," the strategy notes.

Distributed network manager

"One major benefit of 5G is that it can be deployed using commercial servers in any one of a large emerging ecosystem of radio access network, or RAN, providers — all with easy-to-use management tools," said Paul Battaglia, vice president of public sector for [Druid Software](#). "Whether on a base or a command post on the battlefield, Druid has made the management of 4G and 5G cellular networks simple with our distributed network manager (DNM)."

DNM allows the users to fully manage edge cores, connected through a single pane of glass, while also allowing them to control device management. That means they can provision devices across an entire command's 5G cores. It also provides configuration fault and key performance management characteristics of all the packet cores network packets.

"Core software is a fundamental part of the 5G architecture and is responsible for routing, forwarding and managing traffic data between the mobile devices and external networks," Battaglia said. "Druid's core is one of the major technologies focused on simplifying 5G and exploiting its benefits."

These cores are scalable, can be deployed in a backpack or armored vehicle in a contested environment, or provide service to an entire fixed installation, he said. Centralized management means if one core is disabled, soldiers' devices will automatically failover to the next redundant packet core in the vicinity. If one is captured, it can be removed from the centralized database, severing its connections to the others.

Neutral host

One advantage these private 5G cores carry is their ability to leverage the infrastructure of commercial mobile network carriers. That means that when overseas, warfighters can take advantage of the local network infrastructure. When



Druid

Private networks made simple with Raemis™



Multi Operator

extend the coverage of operators with shared RAN



LTE & 5G

Radio agnostic so you can deploy using any RAN



Distributed Networks

Provision, configure and manage networks centrally



Deployment Flexibility

Backpack, vehicle, fixed environment, cloud & more

Find out more at www.druidsoftware.com

deployed in places where traditional network coverage doesn't reach due to the high cost of infrastructure deployment, challenging terrain, low-population density or remote locations, private 5G cores can extend that coverage. They can do this in a scalable fashion, providing 5G to autonomous vehicles or as a separate guest network on a military base.

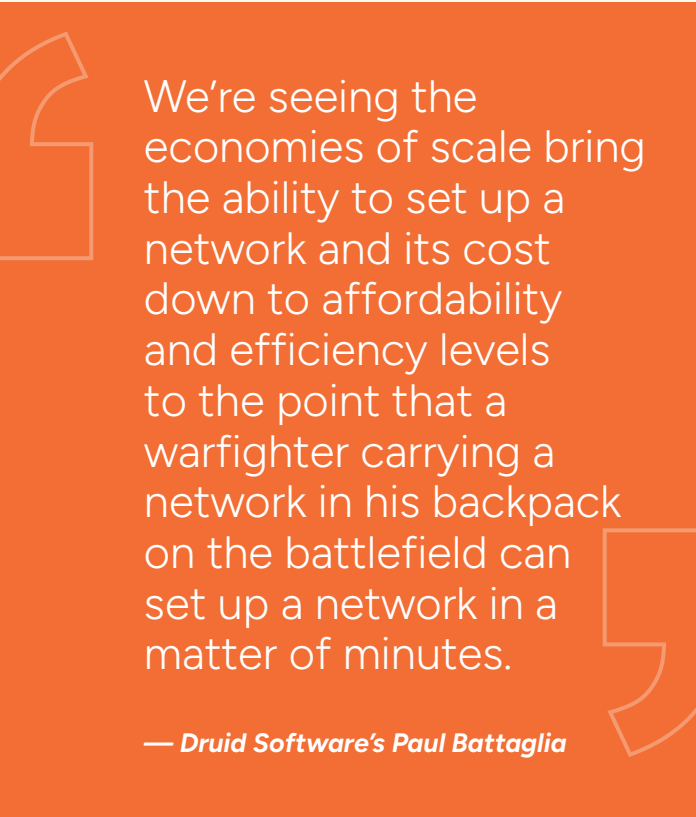
The Druid Raemis Neutral host allows DoD to take advantage of both commercial cellular providers' infrastructure, as well as the Citizens Broadband Radio Service spectrum owned by the government, while meeting DoD's requirements for access control, safety and security.

Network slicing

Network slicing allows operators of private 5G networks to allocate network resources according to the needs of the mission.

"Network slicing enabled by a 5G private network will unlock important military use cases through the efficient allocation of latency and throughput to designated devices and applications," Battaglia said. "As an example, military logistics will benefit from the improved speed in getting supplies to warfighters through robotics and automated inventory management performed by unmanned government vehicles, drones and other Internet of Things devices."

For example, if a drone is going out to do surveillance, lower network latency may be required to retrieve and analyze the video data to make timely decisions. A private 5G network operator can provision more resources to that mission to achieve that lower latency.



We're seeing the economies of scale bring the ability to set up a network and its cost down to affordability and efficiency levels to the point that a warfighter carrying a network in his backpack on the battlefield can set up a network in a matter of minutes.

— *Druid Software's Paul Battaglia*

Ease of setup

The first experiments with DoD smart warehouses cost millions of dollars and took years to launch the ecosystem. The technology was still new and immature. Now, it can be almost immediately set up on commercial off-the-shelf hardware, enabling faster deployments, reduced cost, less dependence on specialized or proprietary equipment and, most important, leveraging a decade of accumulated knowledge and expertise, Battaglia said.

"We're seeing the economies of scale bring the ability to set up a network and its cost down to affordability and efficiency levels to the point that a warfighter carrying a network in his backpack on the battlefield can set up a network in a matter of minutes. That's something that's matured over the last three or four years." 🚀

**For more information, please email enquiries@druidsoftware.com or visit www.druidsoftware.com.
To stay up to date, follow us on [X](#), [LinkedIn](#) and [YouTube](#).**

Q&A with the National Telecommunications and Information Administration's Evan Feinman

The Commerce Department has been pushing for years to ensure every corner of the nation has broadband. One way is through its Broadband Equity Access and Deployment program, or BEAD. The National Telecommunications and Information Administration administers BEAD.

NTIA has been developing guidance for states and territories planning to pay for widening broadband. BEAD Program Director Evan Feinman talked with The Federal Drive's Tom Temin about these efforts.

Federal News Network: Let's start at the beginning, the BEAD program. This idea of broadband throughout the country goes way back, almost to the Clinton administration.

Evan Feinman: The federal government has long identified as a priority ensuring that we can get as many Americans as possible online, and the BEAD program is a real capstone to that work. This program, which was created by the bipartisan infrastructure law, is a \$42.5 billion enterprise that is a partnership between NTIA in the Commerce Department and the various 56 states and territories that are eligible for these funds. And it is the goal of this program — and one that we will realize — to ensure that every single American, home and business has access to an affordable, reliable, high-speed internet connection.

Federal News Network: Hasn't broadband organically spread exponentially throughout the country?

Feinman: In many parts of the country, it has. And, in many parts of the country, it is not.

There are over 8.5 million Americans who have no access to the Internet and tens of millions more who are underserved as opposed to unserved, whose access to the internet is too slow to make meaningful use of many of the different opportunities that folks can take advantage of when they have a good, reliable, robust internet connections.

This program is really designed to solve that problem. Underlying the gap is a fundamental math issue. It costs the private sector about the same amount of money to string a mile of fiber in a dense urban area as it does out in parts of the country that are rural and more sparsely populated. The difference is you might get thousands of subscribers along that mile in a dense urban area. And so it makes sense for the private sector or even a nonprofit or cooperative organization to expend that capital to then bring in that additional revenue.

There are over 8.5 million Americans who have no access to the Internet and tens of millions more who are underserved as opposed to unserved, whose access to the internet is too slow to make meaningful use.



Evan Feinman, Director,
Broadband Equity Access and
Deployment Program, National
Telecommunications and
Information Administration

But once density drops too low, it no longer makes sense to invest that capital. What we're doing in partnership with the private sector and working hand in hand with our states is closing that gap, backfilling that capital gap so that it makes economic sense for an internet service provider to build and then operate network even where the number of American subscribers that they could get may be too low to repay directly that entire capital cost.

Federal News Network: How does this work then from a program standpoint? I'm a county, I'm a territory, or maybe I'm a tribal leader and I want to do this. Do I select the provider and then apply to NTIA for a grant to pay them?

Feinman: Let me answer in specific, and then I'll back up a second and talk through the structure of the program.

The short answer is, if you are a local government or a tribal government, you do have the opportunity to select a partner ISP and bring forward a plan to connect the citizens within the boundaries of your polity. Every tribal and local government has that opportunity by right in the context of this program.

But the structure of this program is significantly different from the structure of prior federal efforts. First and foremost, we are making grants only to the 56 states and territories. Our program makes a grant to the state. And we'll say "state" here for simplicity, although states and territories is always what we mean. Each state will then subgrant those funds out to internet service providers according to a plan that they have written and had approved by NTIA. Then, those subgrantees will build each of these projects.

And so internet service providers may bring their own projects to the state as well as local and tribal governments may bring projects to the state. The state then has to score those projects according to a scoring rubric that was laid out in the state's initial proposal to NTIA. The winners of those bids next detail what states will get in their final proposals. Upon approval of that final proposal by NTIA, then construction begins, and these networks will be built.

The really critical thing that's different about this program versus prior federal efforts is, again, the requirement that the state broadband office, the implementing agency at the state level color in the whole map. We want to see every unserved and every underserved location that's been identified by the state with a proposal to serve it. And we've offered states a variety of different ways to approach that question.

Federal News Network: But there's lifecycle to these networks. There's the laying of cable, that's specialized work, and you have to have infrastructure for all of that. Then there's the ongoing operation of the network, making sure the wire is hot, so to speak, the fiber, whatever. And then there is the revenue side to keep the network up to date because things break.

In my neighborhood, there's all these little boxes with holes in the ground and there always somebody digging in there and doing something. So how does this operate over the long term once the capital initially is done of laying the cable and the connections?

Feinman: There are a raft of obligations that the subgrantees undertake, which include offering a low-cost service option for low-income Americans, which include maintaining certain technical characteristics of the network to ensure that they remain useful for the customers at the end of the road — and a series of commitments to the reliability of those networks as they're operated.

What we've done is we've built a program that gives states very wide guardrails to chart

their path and a lot of tools to ensure that they're building the right network for the right circumstance. It is the primary thrust of the program to build as much fiber optic connection as possible.

Fiber is the most scalable, most futureproof technology that we have to connect citizens. But the program will also wind up investing in a lot of wireless technologies. And we've just announced our alternate technologies approach, which details the ways by which those locations that are their most remote, the most challenging to serve, may be served through low-Earth orbit satellites or through unlicensed fixed-wireless connections, which can still offer in certain circumstances really the best way to get folks connected and offer a high-quality connection.

Federal News Network: That's a different architecture. You have to have the download station and then a way of distributing what comes from the satellite to the local people. So there's a wired and an antenna piece of it, correct?

Feinman: Well, there are two different ways that those satellite connections can work. There is the model that you've described wherein you have a local downlink station and then a local wired network or wireless network that feeds off of that.

There are also low-Earth orbit networks that serve direct to customer. And so the customers have a small dish, and they're able to access that constellation of low-Earth satellites. Again, those are a good connectivity solution for those remote locations to which we can't get a terrestrial connection.

The reason that those don't work everywhere is because of the capacity within those networks. It is simply not the case that those sorts of networks could serve all Americans who are in need of service right now. And that's why we're building out a wide variety of different technologies to make sure that we're using the right solution to solve the problem in each different area in which we find the issue.

Federal News Network: Are there any areas where maybe it's marginal, a certain suburb that might be low income and you could just go to the big ISPs and say, "Come on, guys. Just put it out there."

Feinman: I encourage any ISP to be as aggressive as they can in pursuit of expanding their network to people who are in need of it. But our experience and what prior efforts and early returns from this program are showing is that this model works, and that by offering up subsidy to help the private sector build to reach new customers, the private sector is very interested in doing that. And we support the states in their approach. And the states will, I'm very confident, attract enough partners to get to 100% coverage.


Federal News Network: If you look at agriculture, to take an example of something rural that is technologically intensive nowadays, clearly farmers need broadband because of

the irrigation technologies. The foot-by-foot tailoring they can do to their land treatment has revolutionized farming. And so for them, the devices needed to do that, the GPS stuff, the irrigation equipment, the pad you put in your combine are all part of their capital expenditures. What about poor Americans such that you might spend a certain sum for a local area, but then a phone is \$800 or some decent tablet to take advantage of it is beyond the reach of this program and also beyond the reach of those people's personal budgets?

Feinman: We want to make sure that folks have access to an affordable, reliable, high-speed Internet connection. And so one of the first ways that this program, which is an infrastructure program first and foremost, is attacking that problem is by making a requirement of receipt of funds that a low-cost service offering is offered. That service offering is defined by the state in which a person resides and been approved by NTIA.

We thus far have 55 of the 56 states and territories with approved plans. They are still working within that context, but there is also going to be an opportunity in a set of states to go further.

We divvied up the \$42.5 billion pot among the various states and territories on the basis of need. If a state is able to finish its infrastructure



We are on time and on track to connect every American to that affordable, reliable, high-speed internet service.

— NTIA's *Evan Feinman*

mission under budget, it may then use the remaining funds within its allocation for a wide variety of digital opportunity and digital equity programing, which could include device provision. It could include digital literacy classes. It could include explicit connected agriculture programing or telehealth programing or additional infrastructure to further harden or make resilient the network or expand other network capacities.

All of those are options that we're in dialog with states on now. And we're excited to see what the creativity and commitment to service all 56 of our state and territory partners bring us in that category as we move forward in the program.

Federal News Network: Has any money actually moved out yet for services? Or have you just approved the plans and begun divvying up the funds?

Feinman: Where we are in the process right now, we are on time and on track to connect every American to that affordable, reliable, high-speed internet service. Broadly, under the Biden-Harris administration, thousands of homes and businesses have already been connected. We in the BEAD program have already obligated funds to 55 of 56 territories.

It is now for the states and territories to set about their subgrantee process. And so that is underway in a handful of states and will continue to initiate in the remainder over the coming year. We need them to work with the private sector to stack up those projects to ensure coverage to every single location.

This is by design, a state led program. Some states are really sprinting out to the fore. Other states are taking a more deliberate approach. Both have arguments to commend them. And we're excited to work with states in the manner in which they want to work on this program. We're really, really, really quite pleased to see the progress moving forward. 🏁

How private 5G networks make AI at the edge practical, secure

Every enterprise, whether a private sector company or a federal agency, has more data about its own operations than it has the capacity to meaningfully use.

Vijay Kesavan, senior engineering manager at [Intel](#), calls this “dark data,” and said that while

the desire to leverage this data is what’s driving the rapid adoption of artificial intelligence, two fundamental barriers have stood in the way of harnessing AI to truly leverage it.

First, AI requires the processing power of the cloud, which means enterprises have to move their data in order to get intelligence out of it. This can be costly, and time-consuming. Bandwidth is finite, and the speed at which data travels is limited by the laws of physics, so latency becomes an issue. The second barrier is privacy: Many have been hesitant to store their data in someone else’s infrastructure. That hesitancy only increases for federal agencies whose data includes personally identifiable information, or perhaps even has national security implications.

The answer to both of these barriers, Kesavan said, is to process that data at the edge.

“The key here is you want to process that data where it is generated so that you don’t have issues with moving data, latency of getting the results back, or security of the data,” he said. “In order to do that, what you really need is connectivity. One of the ways that connectivity gets enabled is through 5G.”

The key here is you want to process that data where it is generated so that you don’t have issues with moving data, latency of getting the results back, or security of the data. In order to do that, what you really need is connectivity. One of the ways that connectivity gets enabled is through 5G.



Vijay Kesavan, Senior Engineering Manager, Intel

Connectivity at the edge

If you want to do the compute closer to where the data is gathered, you still need connectivity. Putting the intelligence to, say, perform facial recognition directly into a camera is prohibitively expensive. So even if that data isn't going all the way to the cloud, it still has to move to the local compute source. That can be accomplished through a variety of means: ethernet cable, Wi-Fi, Bluetooth or 5G.

Wi-Fi requires proximity; if you want to mount cameras on a building to monitor a parking lot, that shouldn't be a problem. But mounting a camera in the middle of the lot, or in the middle of a campus, probably won't work with just Wi-Fi. And running physical cable can cost thousands of dollars per meter. Private 5G networks, on the other hand provide consistent connectivity over a much larger area — and with better security, too.

Securing 5G

"Typically, with cellular technologies, when you're doing wireless communication, you have to transmit data at a certain spectrum on a certain frequency," Kesavan said. "With cellular technology, what happens is nobody can start transmitting at a certain frequency. You need to have access to the specific spectrum to do that."

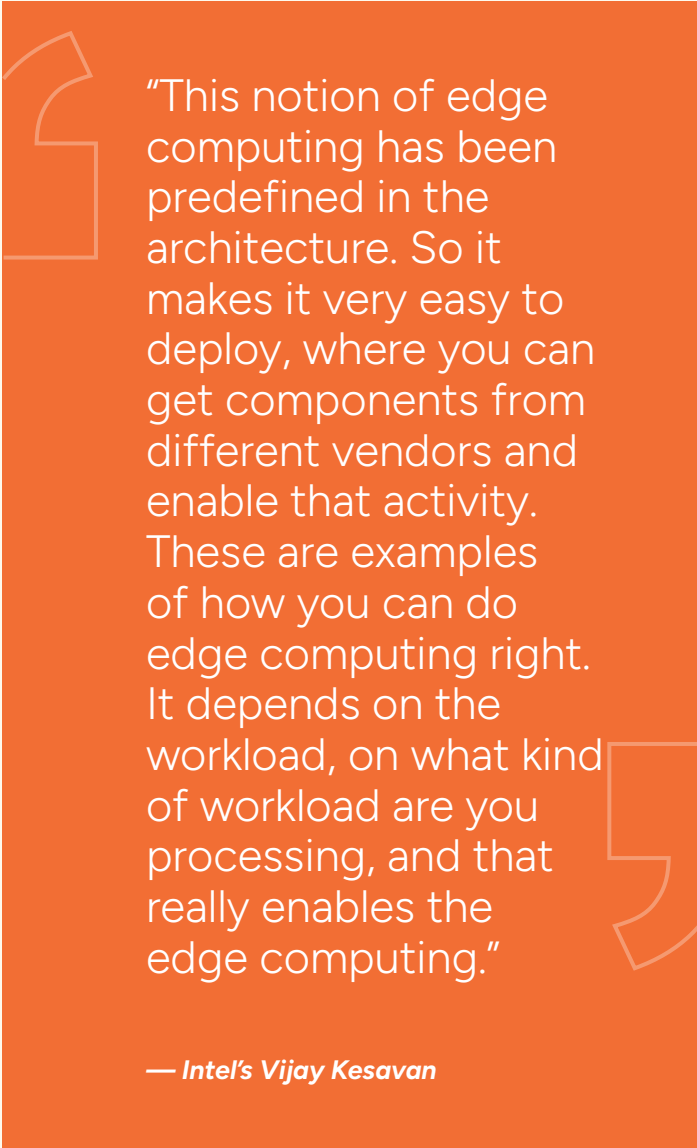
Wi-Fi and Bluetooth operate in what is called "unlicensed spectrum," which means essentially anyone can set up an access point, creating a

massive potential for interference. But cellular technologies like 5G operate on very specific spectrum, so anyone accessing it must be granted permission to do so. That access must be granted to individual devices, so 5G essentially has built-in zero trust. On top of that, 5G has both physical and software layers of security, offering even more protection for the data.

Improved latency

5G's improved latency makes it easier to operate at the edge, enabling use cases that simply aren't possible when data has to be transferred back to the cloud for processing. For example, facilities with automated robots use a closed loop, where a command is sent to the robot, the robot executes the command, then requests another. The tighter latency is in an operation like that, the more efficiently it can be performed. In cases like this, 5G uses ultrareliable low-latency communications (URLLC). So instead of both the robot and the controller requesting bandwidth each time a command is sent, confirmed or requested, URLLC consistently dedicates bandwidth and resources for the duration of the operation. By eliminating the need to continually request and allocate these resources, URLLC tightens latency significantly.

Another use case that benefits from 5G's low latency is augmented and virtual reality. If a soldier is undergoing AR or VR training about tank maintenance, the tank is too big



"This notion of edge computing has been predefined in the architecture. So it makes it very easy to deploy, where you can get components from different vendors and enable that activity. These are examples of how you can do edge computing right. It depends on the workload, on what kind of workload are you processing, and that really enables the edge computing."

— *Intel's Vijay Kesavan*

to fit within the viewscreen of the headset. That means, as the soldier turns their head, the goggles must load more data in order to represent the tank accurately. If that data is coming all the way from the cloud, or experiences other lags in load time, it won't keep up with the speed of the soldier's motion, causing a disconnect between their vision and experience. That usually leads to sickness. Low latency 5G with the data stored at the edge makes AR/VR training like this not only possible, but practical.

"This notion of edge computing has been predefined in the architecture. So it makes it very easy to deploy, where you can get components from different vendors and enable that activity," Kesavan said. "These are examples of how you can do edge computing right. It depends on the workload, on what kind of workload are you processing, and that really enables the edge computing." 🌐



Government Technology Solutions for Positive Mission Outcomes

[Intel.com/Government](https://www.intel.com/Government)



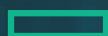
BROUGHT TO YOU BY

carahsoft®

Druid



ERICSSON



Hewlett Packard
Enterprise

intel®