How the US military is becoming open RAN's greatest American ally

The Pentagon sponsored a 5G open RAN test that found Radisys – along with Capgemini, Mavenir and others – provided suitable equipment. Big US network operators, meanwhile, are mostly silent on the topic.

Radisys – along with Capgemini, Mavenir, Signal System Management and Fujitsu – recently walked away with hundreds of thousands of dollars in

winnings from a program sponsored by the US military.

The reason? The companies collectively supplied interoperable 5G equipment using open RAN technology. And Radisys specifically was able to provide the Pentagon with a formal record of the software it used. That software bill of materials (SBOM) is important because it could help soldiers identify security holes that could be used by cyber attackers.

Figure 1:

(Source: Stocktrek Images, Inc./Alamy Stock Photo)

"From my perspective in the Department of Defense, we're interested in that, and really harnessing the possibility of 5G," said Amanda Toman, a Department of Defense (DoD) official in the agency's office of the undersecretary of defense for research and engineering. Toman was speaking in a video about the DoD's ongoing "5G Challenge" program, hosted by the NTIA.

"The promise of what it will provide to the [defense] department, and to the country, is really valuable," Toman said.

Broadly, the situation is noteworthy because the US military, under the auspices of the DoD, has been loudly touting the benefits of open RAN technology. Further, it has put a substantial amount of money – $3 million – toward a 5G Challenge program that is designed to prove out how open RAN technology could create interoperable connections among 5G networking components.

"This 5G Challenge is unique in its extensive and rigorous testing for open RAN interoperability, hardware-software integration and performance benchmarks so that service providers can choose the best-of-breed

solutions with open interfaces for their 5G networks," said Radisys' Ankur Sharma, the company's associate VP of product management and strategy, in a release.

Staying quiet

The big US wireless network operators, in contrast, have remained mostly silent on the open RAN topic. Although Verizon, AT&T and T-Mobile officials have signaled interest in open RAN – and some have admitted to testing the technology – none has yet embarked on any concrete public rollouts, nor has any committed to firm open RAN deployment goals.

That's striking considering US government officials involved with the 5G Challenge program believe open RAN technology has the opportunity to make 5G networks more secure, more efficient and, potentially, cheaper.

"You've got some large mobile operators that are providing systems that are pre-packaged, that come in one standalone stack, there's proprietary software that ties those components together, and if something breaks, you have to go back to that vendor," explained Toman, with the DoD.

Open RAN, according to DoD and NTIA officials, can change that.

Open RAN "facilitates different vendors being able to come in and play for the different pieces" of a network, said Julie Kub, an official with the NTIA's Institute for Telecommunications Sciences (ITS) and the head of the 5G Challenge program. NTIA's ITS division – along with CableLabs – is handling the open RAN testing portion of the program in the agency's Boulder, Colorado, offices.

Seeking a 5G winner

The DoD's 5G Challenge started in 2021 to "accelerate the development of

an open source 5G ecosystem that can support DoD missions." That's not a surprise considering the US military's extensive investments into 5G generally and open RAN specifically, including funding 5G networking tests at a variety of US military bases. Indeed, the DoD is eyeing 5G as the glue that might potentially tie together all of its communications – in order to connect "sensors with shooters across all domains, commands and services."

according to a National Defense article A new DoD research project will look at ways for the US military to use other countries' 5G networks, including those that might be considered insecure.

But the DoD, like many wireless network operators, doesn't want its 5G future to be tied to proprietary, tightly integrated systems supplied by just a handful of vendors. That's why it put $3 million into an NTIA-managed challenge program designed to prove the multi-vendor capabilities of open RAN technology. That program included tests to integrate subsystems from five different vendors: user equipment, radio unit (RU), distributed unit (DU), central unit (CU) and core.

"In true plug-and-play fashion, contestants approached network integration with no prior experience interoperating with their fellow contestants' subsystems," according to the NTIA. "The 5G Challenge provided a rigorous five-week schedule for contestants to work through diverse issues, from 3GPP software options to discrepant hardware."

The NTIA announced the winners of its testing earlier this month, with each receiving $150,000:

CU: Capgemini Engineering, Mavenir Systems and Signal System Management

RU: Fujitsu Network Communications, Mavenir Systems

"NTIA's cutting edge research at ITS, in partnership with federal spectrum users like the Department of Defense, is driving evidence-based policy decisions," NTIA chief Alan Davidson said in a release. "The success of the 5G Challenge will help foster a resilient, competitive, and innovative 5G supply chain, both here at home and around the world."

The NTIA said the rules, location and details of its 5G Challenge Final Event will be released in early 2023.

Related posts:

US military expands 5G testing to include AR, spectrum sharing and open RAN

DoD eyes 'challenge' designed to promote open source 5G

Pentagon puts 5G at center of US military's communications future

— Mike Dano, Editorial Director, 5G & Mobile Strategies, Light Reading | @mikeddano