How Telework Made These Federal Agencies More Secure

Defense agencies tackled intricate cybersecurity challenges to prepare for remote work.

Kate Macri
Fri, 08/07/2020 - 13:53

Many federal agencies scrambled to adjust their cybersecurity strategies while shifting to remote work in March at the beginning of the coronavirus pandemic. But some federal agencies, like the Defense Logistics Agency (DLA) and Defense Contract Audit Agency, found telework helped them improve their cybersecurity posture.
Linus Baker, cybersecurity director for the DLA, said the agency reduced its cyber attack surface by half since the beginning of the pandemic.

“From a cybersecurity perspective, I want to stress our virtual desktop infrastructure,” he said. “More than half of our users are on user-managed devices. Those are never seated on our network, they're not endpoints that provide an attack vector for an adversary, so by that perspective, we've lessened our attack surface by more than half. We gained a benefit there, and an efficiency perspective in executing the agency's mission.”

Baker said DLA already had a reliable telework strategy in place before the pandemic, which streamlined the mass shift in March.

“Most of the challenges we've faced have been mostly administrative, with users who unfortunately weren't or aren't able to telework,” he said at a FedInsider webinar last week. “We had some issues with user accounts because of the timeframe for logging in. But significant challenges? I would say no because we were poised for this given our large telework presence. In many ways DLA was ahead of the game.”

Anita Bales, director of the DCAA, said the agency was also “well positioned” for the shift to 100% telework because 30% of the agency’s employees already teleworked before the pandemic.

DCAA initially struggled to ensure its remote employees had enough bandwidth, but DOD helped sort that out relatively quickly, Bales said.

The DCAA also didn’t face any major cybersecurity challenges when shifting to telework, largely because it was already familiar with typical telework challenges like ensuring VPN security.

“With our VPNs, we made sure before we went into all of this we had all our security patches up to date and deployed a new patch right when we were going out,” she said during the webinar. “We would shut one [VPN] down and operate off of the other until we had all the patches in place.”
Telework strategies aside, Bales said employees’ good cyber hygiene is fundamental to any organization’s cybersecurity strategy, especially while working remotely.

“Make sure you're not opening emails you're not familiar with,” she said. “Remember you are a DOD employee using your government computer — make sure you don't use anything outside of our VPNs. Bad actors know we're in a virtual environment, and they're going to try to take advantage of that.”