

How the need for teleworking is speeding up the Pentagon's IT overhaul

By Sarah Cammarata

04/30/2020 12:00 PM EDT Updated: 04/30/2020 06:10 PM EDT

The coronavirus pandemic — which has forced hundreds of thousands of defense employees and contractors to work from home — has given a much-needed shot in the arm to military plans to upgrade their IT backbones.

In mid-April, Pentagon Chief Information Officer Dana Deasy assembled [a team of top IT officials](#) to handle the “expanded need for massive telework capabilities.” And the military services have sprung into action as well.

The Marine Corps, for example, first responded to the pandemic by expanding workers’ access to reliable and secure networks. The service has “drastically increased” service member’s ability to work from home and access their email through Outlook Web Access, said Capt. Héctor Alejandro of the Marine Corps Forces Cyber Command.

Within a few days in March, the number of simultaneous users on their safe, remote networks jumped from 12,500 to 60,000, Alejandro said.

“Efforts to deliver a secure, cloud-based capability to our Marines and civilian workforce have been accelerated by the need to work from alternate locations,” said spokesperson for the Marine Corps’ Deputy Commandant for Information Maj. Sharon Sisbarro in a statement.

Meanwhile, the Army’s network operators, who defend the network for more than a million Army customers worldwide, are “working around the clock” to ensure it’s secure, Army spokesperson Jason Waggoner said.

And while a number of IT-related priorities are not necessarily new, “what is new is the opportunity to take some calculated risks in order to rapidly accelerate next generation capabilities ... we recognized early on that what is needed are network enhancements.” Lt. Gen. Bruce Crawford, the Army chief information officer, said in a statement.

William Marion II, Air Force deputy chief information officer, noted some of the service's key priorities, such as the Office 365 environment, have now been sped up. “All of those were already in the works ... it does influx some real priorities to get over the hump in some areas to really take these to the next level,” Marion said in an interview.

The Defense Department, which released a [new cloud environment from Microsoft](#) to make the surge of workers at home more manageable, has aided collaboration among the Air Force’s members, Marion said.

Before the pandemic, the Air Force had just under 10,000 users teleworking on any day. That number has swelled to more than 150,000 concurrent users on virtual private networks, marking a 1,700-fold increase since the outbreak began, Marion said.

The Army now has 800,000 members who can telework using the DoD’s networks and “overall demands are increasing daily,” service spokesperson Lauren Brennan said.

The Army, with about 70 percent of its workforce teleworking, has seen a 400 percent increase in network access and data/voice capacity, Brennan added.

The Coast Guard, meanwhile, has taken steps amid the pandemic to [start working on its IT overhaul agenda](#) and harden its systems using funds provided under the Coronavirus Aid, Relief, and Economic Security Act.

Commandant Adm. Karl Schultz told POLITICO in a recent interview that more than \$60 million provided the service a “good shot in the arm” to put toward capacity and capability on information technology management.

“This was a place where we've been conditioning the battlespace a bit on this conversation about the Coast Guard’s failing IT infrastructure. I think it was well-received,” Schultz said.

Funding provided in the coronavirus relief package, as well as money in the fiscal 2021 budget, will help address the connectivity for the services’ cutters, Schultz added. Tech refreshes, among other projects, are some things that can now be accelerated, the top admiral said.

Cyber attacks

The time for IT modernization could be overdue, however, amid reports that the Pentagon is facing an uptick in certain cyber attacks.

One of the Pentagon’s top IT officials recently [said the Defense Department has seen a "surge" in spear phishing attacks](#) as its civilian and military workforce has shifted to telework.

And a recent Government Accountability Office report [warned the DoD is significantly lagging in implementing basic cybersecurity practices](#), years after some were set to be completed.

The Air Forces’ Marion said in terms of cyber concerns, “there’s certainly people trying to, whether it’s criminal activity or nation-state, trying to take advantage of the situation.”

However, Alejandro of the Marine Corps said an unintended consequence of accelerating IT modernization and consolidating into one cloud means it's easier to defend one area from attacks than several.

“Not only does this decrease the operating cost long-term for acquiring new IT and refreshing hardware and software,” Alejandro said. “Any time you consolidate on one type of capability, one type of software ... we have one base that we’re protecting instead of 30 bases, or however many bases we have right now.”