

Navy Cybersecurity Director: 'No Relaxation of Defenses' During Telework Time



Sailors stand watch in the Fleet Operations Center at the headquarters of U.S. Fleet Cyber Command. U.S. Navy ARLINGTON, Va. – The U.S. Navy is maintaining a vigilant cyber watch over its data networks as it balances network security and protecting the health of its Sailors amid the COVID-19 pandemic, a Navy admiral said.

“We’re trying to balance two different priorities,” Rear Adm. Kathleen Creighton, director of cybersecurity in the Office of the Chief of Naval Operations, said during an April 17 webcast that was part of the Navy League’s Sea-Air-Space 2020: Virtual Edition. “One is keeping our Sailors and civilians safe and to enable them to work remotely and second is to ensure operational readiness.”

To register and then watch this Sea-Air-Space 2020: Virtual Edition webinar live online, click [here](#).

Creighton said the Navy has had to go through a big cultural shift from working in offices to “ensuring as many people as possible can work from home remotely.”

She said that, in addition to Defense Department partners, the Navy’s industry partners had taken a “first responder-type approach to helping the Navy” by adding infrastructure to handle the ballooning demand for secure telework.

“We’re trying to balance two different priorities. One is keeping our Sailors and civilians safe and to enable them to work remotely and second is to ensure operational readiness.”

Rear Adm. Katherine Creighton

The admiral cited the need for significant expansion of capacity, the need to maximize collaboration capabilities, and determination of any need to change cybersecurity policy “to ensure we can take advantage of remote telework options.”

She said that “on any given day probably only a few thousand people accessed the Navy’s network remotely ... before COVID-19. Now, we are seeing upwards of 150,000 or more people accessing the network remotely.”

The great increase in telework required an expansion in capacity requirement for laptop computers, mobile phones, iPads and the VPN servers that they connect to as well as an expansion of Microsoft Outlook 365 use. Circuitry also had to be added to handle the increased use of devices as well as more people manning the help desk for the network.

Creighton said the Navy “has been on a road to modernize and to start using more collaboration capabilities, and this crisis has pushed us to roll those out faster. We’re using some temporary capabilities, and we’re looking to accelerate

our permanent capabilities.”

She said the Navy is discovering where the bottlenecks in the network are and fixing them on a piece-by-piece basis. In addition to expanded circuitry, the Navy has been cleaning up user accounts and increasing licenses.

“Every time we increased the capacity, it was used. It filled right up,” she said. “So, the Navy is taking working from home very seriously, trying to protect our Sailors and civilians.”

“Our adversaries in cyberspace know we were doing business differently, so they are responding in kind,” she said, “so we have made sure that anything we have done has not relaxed our cybersecurity standards.”

“There has been no relaxation of any defenses,” she said. “We are securely connecting with that same network from home.”

Creighton said a temporary cloud is being set up to handle a faster roll-out of Office 365.

Looking to the future after the COVID-19 pandemic, Creighton said she believes “there would be a desire to continue a greater level of telework than we saw in the past, so we need to be sure that our network has the capacity to do that, that we have the procedures in place to do it, but most importantly we’re able to do it securely to protect our information and our people’s identity and other things we value as a Navy.”