

NAVAL WARFARE, NETWORKS / CYBER

Navy's approach to cybersecurity is 'wrong,' top info officer says

"We view cybersecurity as a compliance problem. And it is most definitely not a compliance problem," Navy Chief Information Officer Aaron Weis said, arguing the service must shift to a "readiness" focus.

By JASPREET GILL on April 19, 2022 at 2:05 PM



Lt. Christian Asaban views a computer monitor aboard the forward-deployed Arleigh Burke-class guided-missile destroyer USS Fitzgerald (DDG 62) during Multisail 17 on March 8, 2017. (U.S. Navy photo by Mass Communication Specialist 2nd Class William McCann/Released)

WASHINGTON: The way the Navy currently approaches cybersecurity is "wrong," and the service needs to move from viewing it as a compliance problem toward a model rooted in readiness, according to the service's chief information officer.

"Today, I would argue that the way that we do cybersecurity at the Department of Navy — and at the Department of Defense but that's above my paygrade — ... is wrong," Aaron Weis, Navy CIO, said at the Cloudera Government Forum. "We view cybersecurity as a compliance problem. And it is most definitely not a compliance problem."

Instead, the service needs to move toward a readiness model that is measured holistically, he said.

"And when I talk about readiness, I'm not saying it's fleet readiness ... I'm saying it's a model inspired by how we approach readiness," Aaron Weis, Navy CIO, said at the Cloudera Government Forum. "Readiness is something that is a dynamic model ... It is measured very holistically."

RELATED EXCLUSIVE: [MS Teams users at Army Futures Command potentially exposed private info](#)

Cybersecurity through compliance results in risk increases, delayed capabilities, inadequate protection and wasted resources, according to Weis.

The Navy has been working towards its new, holistic model since last November and to that end created a program called Cyber Ready. With the program, the service wants to shift cybersecurity away from rote compliance bureaucracy and towards a "cyber ready" state that enables acquisition speed and better defends the service's information.



AIR WARFARE, SPONSORED

A new approach to speed, scale and efficiency for the industrial base

Radars, EW, EO/IR, space imagery, and microelectronics are brought under one roof for a streamlined approach to common people and factories.

From [BREAKING DEFENSE](#)

The program also seeks to "apply models of currency so that we're not just getting an ATO [authorization to operate] once, but you're continuing to earn and re-earn your ATO everyday through this idea of currency," Weis said.

RELATED: [App Store For Warships: Inside The Navy's Project To Revamp How The Fleet Gets Software](#)

In addition to the currency concept, Weis said, there are several lines of effort the Navy is pursuing to move the service to a more holistic cybersecurity approach, including continuous monitoring with program-driven red teaming and auto-red teaming,

acquisition changes and preparing its workforce.

“And so we’re on a path. This launched last year,” Weis said. “We are on a first set of sprints, a 90-day sprint, where we’re putting the meat on the bones of this idea. And we’re also actively working to identify sets of pilots. And so we’re getting a small number of pilots who are volunteering to go through this and help us learn and it will be a highly iterative approach as we move forward.”



Recommended
Where to find the sights and sounds of Sea Air Space 2024

Check out the photos and flavor of the Sea Air Space 2024 Conference and Exposition.

By BREAKING DEFENSE

Weir also laid out three broad goals the Navy wants to accomplish based on its [2019 Cyber Readiness Review](#): modernize the service’s infrastructure, drive innovation at speed and defend the service’s information “wherever it is.”


“And notably, we did not use the word cyber. I’m of the mind that cyber is probably one of the most overused words in this town, in this industry ... It means everything to everyone,” he said. “And therefore it sort of means nothing. So we have to put a finer point on it. We have to defend our information wherever it lives — at rest, in transit, in the industrial base, in our systems, at the tactical edge. You name it, we have to be able to defend it. And we have not been doing a great job of that in the past as the Cyber Readiness Review articulated.”

Weis’s comments come as the Pentagon ramps up funding in its cyberspace activities and aims to [streamline its vast network infrastructure](#) of non-service-specific agencies.


DoD in its fiscal 2023 request wants [\\$11.2 billion](#) to harden its networks, operationalize zero trust architecture and increase cybersecurity support for defense contractors. The request is an \$800 million increase over its FY21 request.

“We’re also investing to improve readiness in the nation’s cyber force by funding cyber ranges to enable training and exercises in the cyber domain,” Vice Adm. Ron Boxall, director of force structure, resources and assessment for the Joint Staff, told reporters March 29. “Finally, the budget lays the foundation for US [Cyber Command] to have ownership of the mission and resources of the cyber mission force beginning in FY24 as directed in the [FY]22 NDAA.”

Recommended



Where to find the sights and sounds of Sea Air Space 2024



'One pane': Navy seeks standardized C2, data-sharing for unmanned systems

✕ f in ✉

Topics: aaron weis, ATO, cyber readiness review, cyber ready, Navy, navy cio