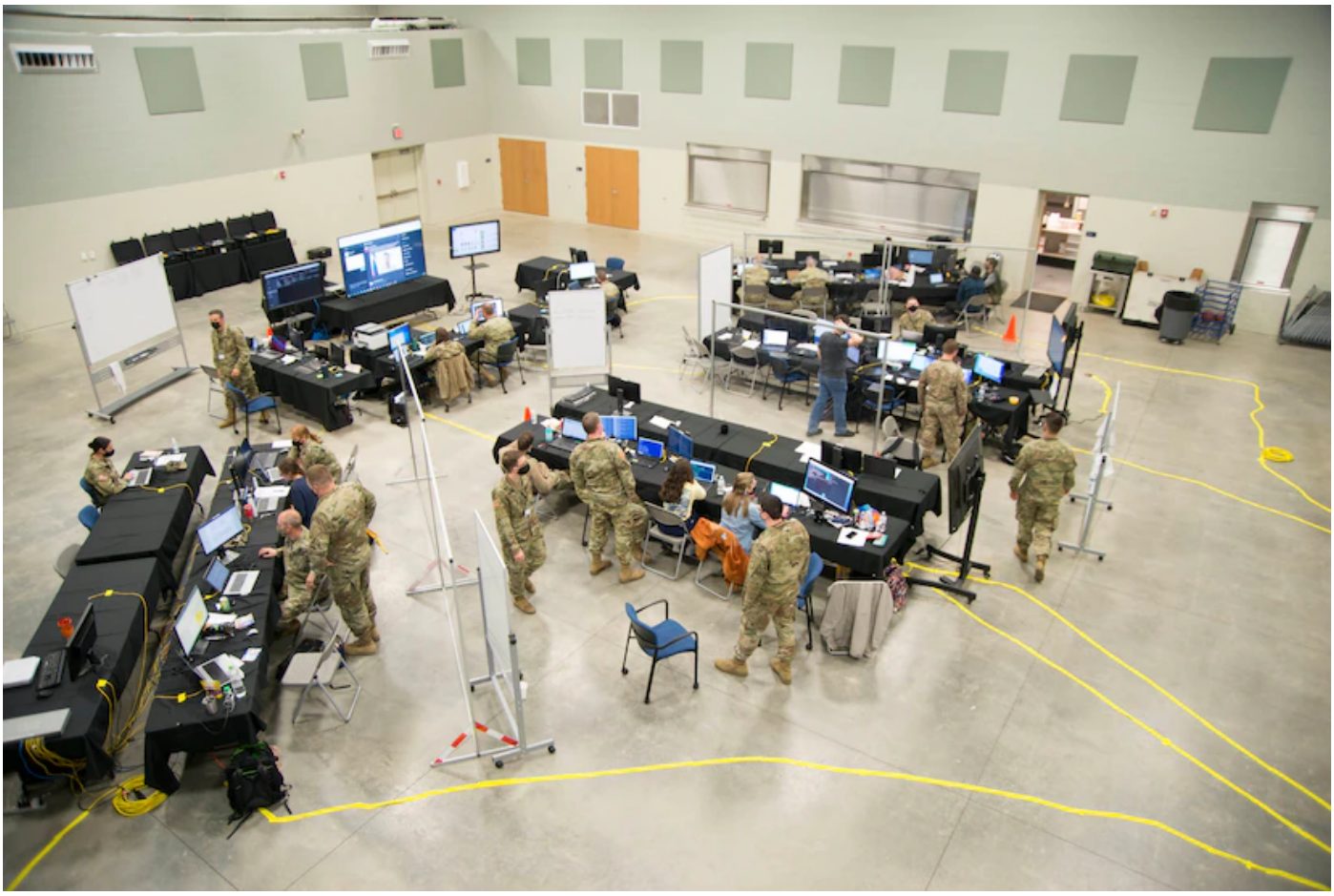
DOD Expands Hacker Program to All Publicly Accessible Defense Information Systems

May 4, 2021 DOD News

Ethical hackers now have many more targets within the Defense Department, DOD officials announced. The department is expanding its Vulnerability Disclosure Program to include all publicly accessible DOD information systems.

The program grew out of the success of the "Hack the Pentagon" initiative that began in 2016. That initiative enabled the Defense Digital Service to offer a "bug bounty" program and engage with hackers. There really was no way for hackers to interact with DOD even if they spotted a vulnerability before this program. "Because of this, many vulnerabilities went unreported," Brett Goldstein, the director of the Defense Digital Service, said. "The DOD Vulnerability Policy launched in 2016 because we demonstrated the efficacy of working with the hacker community and even hiring hackers to find and fix vulnerabilities in systems."



The original policy was limited to DOD public-facing websites and applications. The expansion announced today allows for research and reporting of vulnerabilities related to all DOD publicly-accessible networks, frequency-based communication, Internet of Things, industrial control systems, and more, Goldstein said. "This expansion is a testament to transforming the government's approach to security and leapfrogging the current state of technology within DOD," he said.

The DOD Cyber Crime Center oversees the program. The expansion was the next logical step, Kristopher Johnson, director, Vulnerability Disclosure Program, said. "The department has always maintained the perspective that DOD websites were only the beginning as they account for a fraction of our overall attack surface," he said.

Since the Vulnerability Disclosure Program's launch, hackers have submitted

more than 29,000 vulnerability reports, with more than 70 percent of them determined to be valid, officials said. With the scope expanding, Johnson anticipates the numbers will drastically increase due to the security researcher community discovering vulnerabilities that were previously unreportable.