DOD to Try Out Its Vulnerability Disclosure Program with Contractors

The Defense Cyber Crime Center will launch the program on April 5 in collaboration with the Defense Counterintelligence Security Agency.

Mariam Baksh February 2, 2021

Ivan Cholakov/Shutterstock

The Defense Department's Cyber Crime Center will soon be accepting applications for a limited number of companies within the defense industrial base to benefit from security researchers already working for the department.

"If you're a small to medium sized DIB company and are interested in attending an industry day on Feb. 12th to learn how this free, DoD-provided

capability will improve your #cyberhygiene please send an email to DIB-VDP@dc3.mil for an invite," the center recently wrote in a pair of tweets. "Application window opens after event!"

DOD's Cyber Crime Center already hosts a voluntary cybersecurity program with a collaborative information sharing environment which includes over 720 companies, according to Carnegie Mellon's Software Engineering Institute, which conducted a feasibility study on the expansion of the DOD's current vulnerability disclosure program. DOD sponsored the study by the institute, which is a leader in the vulnerability disclosure coordination space and a federally funded research and development center.

Vulnerability disclosure programs, where security researchers are given safe harbor from prosecution in exchange for identifying how threat actors can exploit a system's weaknesses, are still not present in the vast majority—94%—of Fortune 2000 companies, according to the study. DOD, and more recently the Cybersecurity and Infrastructure Security Agency, have brought such programs to government systems, and related bug bounty programs are popular in mature segments of the private sector. But contractors have unique concerns.

The Carnegie Mellon study recommended a pilot to test how the program would address those, and advised that it initially only be open to 20 companies from across the defense industrial base.

The program will launch on April 5 in collaboration with the Defense Counterintelligence Security Agency and the information sharing environment, the Defense Cyber Crime Center said.

The Carnegie Mellon study includes an appendix: a user agreement they prescribe all participating companies sign to address concerns of both the contractors and security researchers, as well as other stakeholders.

For example, a major incentive for security researchers is making a difference. They want to know that if they identify a vulnerability that threat actors can exploit, it will be mitigated. But timely mitigation requires resources and can fall to the wayside, discouraging researchers.

Under the user agreement, the companies would decide which of their assets would be in scope for the program, but officials within the vulnerability disclosure program, not the companies, would provide the final word on whether a vulnerability has been addressed. The study also points out gaps that need to be addressed, one of which is the determination of consequences for companies that don't meet timing requirements for addressing vulnerabilities.

Another term of the proposed user agreement is that agency records, which may include qualifying information received from non-federal entities, are subject to the Freedom of Information Act. But the government promises to protect any proprietary information researchers may come across, and to only use such information in the case of national security needs.

The user agreement also makes clear that "a reported vulnerability under the Program is not, in and of itself, considered to be a cyber incident and does not require a mandatory report," pursuant to current Defense federal acquisition regulations. "However, the Participant's review and efforts to remediate a reported vulnerability may lead to the Participant discovering reportable cyber incidents which may trigger a contractual reporting requirement."

Altogether, the Carnegie Mellon study expects that a tracking system the program will use—the Vulnerability Reporting Management Network—will provide valuable insights about the sector's security, provide early warning to participating companies, and could provide a model for broader public-

private collaboration.

“One of the true values of this program will be in the longitudinal reporting of trends and alerting of critical and high vulnerabilities across DIB companies,” it reads. “While novel in the public-private information sharing environment, the DoD’s VDP program can provide a useful exemplar for a successful transition into public-private vulnerability sharing cooperation.”