wiley

NEWSLETTER

DOD Piloting a Private Contractor Vulnerability Disclosure Program

October 2020

The U.S. Department of Defense (DOD) continues to pursue innovations in its approach to security vulnerabilities, building on its earlier Hack the Pentagon program and recent moves by the U.S. Department of Homeland Security (DHS) to require federal agencies to adopt and expand vulnerability disclosure programs. Given the relationship of federal agencies and the contractors that support their missions, this suggests increasing obligations loom for contractors.

Presently, DOD is seeking input on a pilot program for vulnerability disclosure and remediation in contractor networks. The Defense Industrial Base-Vulnerability Disclosure Program (DIB-VDP) Feasibility Study public comment period will be open until December 6, 2020.

This request for information flows from a July 2020 study from the Software Engineering Institute at Carnegie Mellon University. "VDP programs use security researchers from around the world to identify vulnerabilities (vulnerability discovery) and provide a proof-of-concept exploit for that specific vulnerability." According to Carnegie Mellon, DOD has been looking to expand its work and information sharing with the private sector. DOD's "Cyber Crime Center (DC3) and the Defense Counterintelligence and Security Agency (DCSA) signed a Memorandum of Agreement (MoA) to discover new ways to share information security data. One of the areas of cooperation between the two organizations was to discover how to share vulnerability data with Defense Industrial Base (DIB) companies."

After considering the MoA and related issues, Carnegie Mellon concluded that "[t]he most effective method of sharing vulnerability data between DCSA and DC3 is to design and field a pilot program, based on the existing DOD VDP model. The scope of the pilot should

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Government Contracts
National Security

be limited to 20 DIB company participants, under the authority of DCSA and 10 under DIB CS Program authority."

The proposed pilot program appears intended to depend on HackerOne, a private company that helps with security research and VDP management. "DIB-VDP would likely use the commercial company HackerOne (already in use for DOD VDP) to establish the DIB-VDP portal and then manage, which would include posting specific DIB-VDP participant scoping information and hosting ticketing data in a secure manner. However, other platforms such as GitHub could also be employed for certain functions as well, which may reduce costs."

The documents recognize this is a paradigm shift for many companies. VDPs bring challenges to companies, and require careful planning and considerations about scope, liability, and more, as we have previously explained. DOD's original Hack the Pentagon effort in 2016 involved 1,400 hackers and discovered 138 unique vulnerabilities. DOD's Cyber Strategy prioritizes "crowdsourcing opportunities to identify and mitigate vulnerabilities more effectively" and VDPs have become fashionable with some members of Congress, who are looking to encourage contractors and others, such as makers of Internet of Things devices, to adopt some variants of VDP. For example, Senator Mark Warner (D-VA) has repeatedly called for DOD to take more steps and for additional legislation in this area.

Whatever DOD does here is likely to inform future work by other agencies and should signal to the broader contracting community the government's sharpening interest in how they handle and manage vulnerabilities. These programs and efforts raise challenging questions, including around scoping and definition of vulnerabilities. Not all vulnerabilities are created equal and not all can or should be patched. Some researchers have observed out that "[i]n aggregate, over all the software products we analyzed, about 15% of the known vulnerabilities have been exploited in real-world attacks." Varied mitigations may be appropriate in a risk-based approach to enterprise, device, and service security.

DOD recognizes that there will be growing pains. "The DIB-VDP Pilot will invite researchers to try to detect weaknesses and vulnerabilities in [private] systems. Participants may need to be educated as to the value of this exercise." The private sector participants "may not be well educated on vulnerabilities and establishing priorities in their mitigation strategy. DOD VDP lists each vulnerability that comes into the program as a 'Critical', 'High', 'Medium', 'Low', or out of scope. These terms will need to be adequately communicated to participant companies since they are subjective terms by nature. It is very important for both the DIB-VDP and the participant company be 'on the same page' in the prioritization scheme."

In addition, companies that participate in the pilot will take on obligations, including agreeing "to provide safe harbor for researchers who abide by the DIB-VDP pilot rules of engagement and scoping instructions" and agreeing "to perform good faith efforts, in accordance with the DIB-VDP Terms of Service Agreement, to mitigate DIB-VDP researcher reported vulnerabilities within their infrastructure."

The documents pose numerous questions about implementation challenges. And the description does not address costs or reimbursement for participation or for the technical work that may be needed to assess and mitigate vulnerabilities.

Contractors can expect VDPs to expand throughout government and should look to this Pilot as a bellwether for what to expect when other agencies move to implement their own programs. If the DIB-VPD poses concerns or would be challenging if applied to your organization, it may be prudent to submit comments or share your concerns. As noted, comments are being accepted through December 6, 2020.