DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM (DIB-VDP)

DC3 ESTABLISHES DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM (DIB-VDP)

The Department of Defense (DoD) Cyber Crime Center (DC3) and Defense Counterintelligence and Security Agency (DCSA) have established a fully operational vulnerability disclosure program supporting the Defense Industrial Base (DIB). Following a successful 2022 pilot, which focused on delivering a DoD/ DC3 vulnerability disclosure capability to the DIB, this strategic alignment further enhances DC3 and DCSA support to the DIB in the vulnerability, analytical, cybersecurity, and cyber forensics domains. This program aligns to and addresses national-level cybersecurity strategies and policies, such as the 2022 National Defense Strategy and the 2023 National Cybersecurity Strategy.

HOW WE GOT HERE: DIB-VDP PILOT

The DIB-VDP Pilot was a 12-month voluntary event established collaboratively by the DC3 DoD Defense Industrial Base Collaborative Information Sharing Environment (DCISE), DoD Vulnerability Disclosure Program (VDP), and DCSA. The DIB-VDP Pilot was born out of the desire to deliver the lessons learned by the DoD VDP to DIB companies. On 26 November 2019, DC3 and the DCSA signed a Memorandum of Agreement to discover new ways to identify and remediate vulnerabilities in the DIB. Another area of cooperation between the two organizations was to disclose vulnerability information with DIB companies in the DIB-VDP.

Since 2016, the DC3's DoD VDP is the single focal point for receiving and validating vulnerabilities reported on the Joint Force Headquarters-DoD Information Networks. Validated vulnerabilities are coordinated with internal DoD asset owners tasked with the primar y responsibility for defending DoD's enterprise data systems. VDP leverages crowdsourcing vulnerability discovery as a cost-effective way to reduce organizations' cybersecurity risk by providing a "hacker's view" of its external attack surface.[1]

DC3's DoD VDP performs a coordinated vulnerability disclosure process of ingesting information from designated vulnerability researchers, coordinating the sharing of that information to relevant stakeholders for the purpose of timely remediation, then using non-attributional disclosure of validated vulnerabilities and their mitigations.

Leveraging this proven enduring VDP model for DIB-VDP implementation is the most effective means of encouraging vulnerability discovery for DIB company's publicly accessible information systems. This no-fee, voluntary program enables timely vulnerability mitigation for DIB companies at a much earlier point than traditional vulnerability management efforts alone.

DIB-VDP PARTNERSHIP

DCSA is a partner in the DIB-VDP. The DCSA performs similar sharing opportunities with the National Industrial Base companies that maintain classified contracts, cleared personnel, and operate classified systems, housing national and DoD data. DCSA is responsible for Personnel Vetting and Critical Technology Protection, providing oversight to about 10,000 cleared companies, roughly 13,500 facilities, under the National Industrial Security Program. While it includes DoD and DCISE's collaborative partnership with 1,200+ DCs and USG agencies, the DCSA also oversees cleared industry members for 33 other U.S. Government organizations, ensuring adequate protection of facilities, personnel, and associated IT systems from attacks and vulnerabilities. Through this program and partnership, DC3 seeks to build upon and improve the combination of policies, requirements, services, pilots, public-private collaboration, and interagency efforts to combat the complex, ever-evolving cyber threats facing the DIB.

[1] DoD Instruction 8531.01 - DoD Vulnerability Management

DoD CYBER CRIME CENTER AND
DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY

AFOSI.DC3.DIB-VDP@us.af.mil