A FEDERAL CYBER CENTER

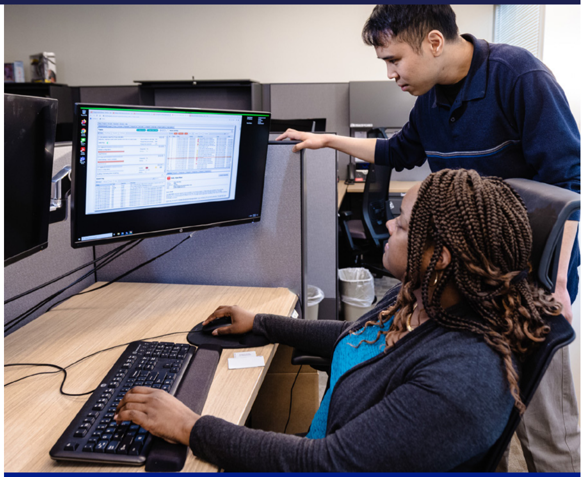
DoD CYBER CRIME CENTER

Vulnerability Disclosure Program (VDP)

Established in 2016 by the Secretary of Defense, the **Vulnerability Disclosure Program (VDP)** operates to strengthen the security of the DoD Information Network (DoDIN) by providing an additional layer for the defense-in-depth cybersecurity strategy.

VDP functions as the single focal point for receiving vulnerability reports and interacting with ethical crowd-sourced cybersecurity researchers supporting the DoDIN.[1] This improves network defenses and enhances mission assurance by embracing a symbiotic operational relationship with private-sector ethical researchers. January 2021, the DoD VDP scope was officially expanded from public-facing websites to all publicly accessible information systems throughout the DoD. This broadens the protection for the DoD attack surface and offers a safe harbor for researchers while providing more asset and technology security. The success of the program relies solely on the expertise and support of the security researcher community, and the program's success contributes to the overall security of the DoD.

DoDIN information technologies, services, and systems provide critical capabilities to all military service members, their families, veterans, DoD civilians, and contractors.



VDP drives increase in the cyber hygiene of the DoDIN, with the objective of ensuring that the DoD can accomplish its mission of defending the United States of America.

over **50,000**

Vulnerabilities Submitted (since launch)

over **5,500**

Participating Researchers (since launch)

over **28,000**

Mitigated Threats (since launch)

[1] DODI 8531.01 DoD Vulnerability Management Section. 2.11

CAPABILITIES

The DoD Vulnerability Disclosure Program:

- As a key component of the National Cyber Strategy, Pillar II, promotes full-lifecycle cybersecurity through the use of coordinated vulnerability disclosure, crowdsourced testing, and risk assessments that improve resiliency ahead of exploitation or attack
- Enhances the partnership between DoD and the computer security researcher community, building a positive feedback loop to enhance the security of the DoD through the speedy discovery and remediation of vulnerabilities
  - Reduces the elapsed time from discovery of a vulnerability to notification of the system owner to successful mitigation of the vulnerability
  - Provides an open channel and legal safe harbor for the discoverer of the vulnerability to report it to DoD
  - Aligns with ISO 29147:2018 and ISO 30111:2019

AWARDS

2019 DOD CIO Award Winners–Cybersecurity Team

We are truly honored to be selected amongst a very competitive pool of nominees for the DOD CIO award for Cybersecurity. Winning the DOD CIO Award demonstrates how the importance of the DOD Vulnerability Disclosure Program (VDP) is to protect the DOD Information Network (DODIN) as another layer to any effective defense-in-depth strategy using the vast capabilities of the white-hat researcher community.

DoD CIO ANNUAL AWARDS WINNER CYBER & IT EXCELLENCE

2022 DOD CIO Award Winners–Defense Industrial Base Vulnerability Disclosure Pilot (DIB-VDP) Team

Winning this award demonstrates the importance of leveraging the lessons learned from the VDP program to protect the Defense Industrial Base (DIB). The DC3 DIB-VDP team would like to thank the Defense Counterintelligence and Security Agency (DCSA) for their collaborative effort on the pilot and our critical partnership with the crowdsourced ethical researchers.

Pub. Date 10 MAY 2024