



DoD CYBER CRIME CENTER (DC3)

Vulnerability Disclosure Program

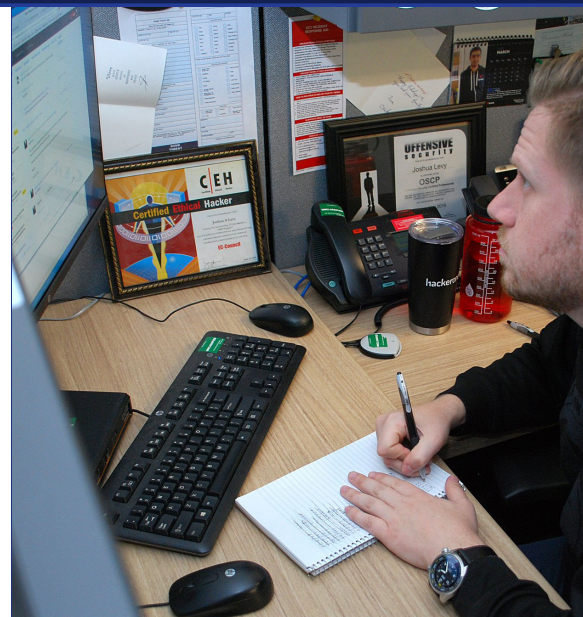
VDP FACT SHEET



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 to the defense-in-depth cybersecurity strategy.

Our mission is to act as the single DoD focal point for receiving crowdsourced cybersecurity vulnerabilities on the DoDIN to improve network defenses and enhance mission assurance, by embracing a previously overlooked yet indispensable resource; private-sector white hat researchers. The success of the program relies solely on expertise and support from the security researcher community which 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. Ultimately, VDP will drive an increase in the DoDIN's cyber hygiene with the objective of ensuring DoD can accomplish its mission to defend the United States of America.



VDP Cyber Intel Vulnerability Specialist validating a submission from our security research community.

“VDP provides the DoD community with an independent, world-class team to identify and help mitigate their Cyber-based vulnerabilities by leveraging capability of ethical hackers from around the world”

—VDP



DoD CYBER CRIME CENTER

VDP-Questions@dc3.mil

410-981-6610 | www.dc3.mil | info@dc3.mil

@DC3VDP, @DC3Forensics
@DC3 Cyber Crime Center



CAPABILITIES

The DoD Vulnerability Disclosure Program:

- Key component of the National Cyber Strategy, Pillar II, by promoting 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 DoDs security through the speedy discovery and remediation of vulnerabilities.
- Reduces the time between when a vulnerability is discovered, when the system owner is notified and when the vulnerability is successfully mitigated.
- Provides an open channel and legal safe harbor for the discoverer of the vulnerability to report it to DoD.
- Facilitates the National Defense Strategy LOE "Build a More Lethal Force" by increasing the resilience of the DoDs cyberspace assets.
- Aligns with ISO 29147:2018 and ISO 30111.

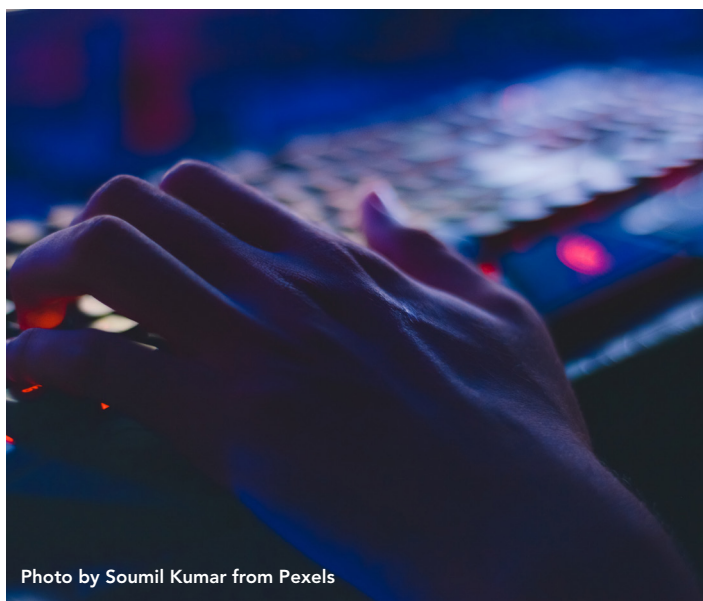


Photo by Soumil Kumar from Pexels

