A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

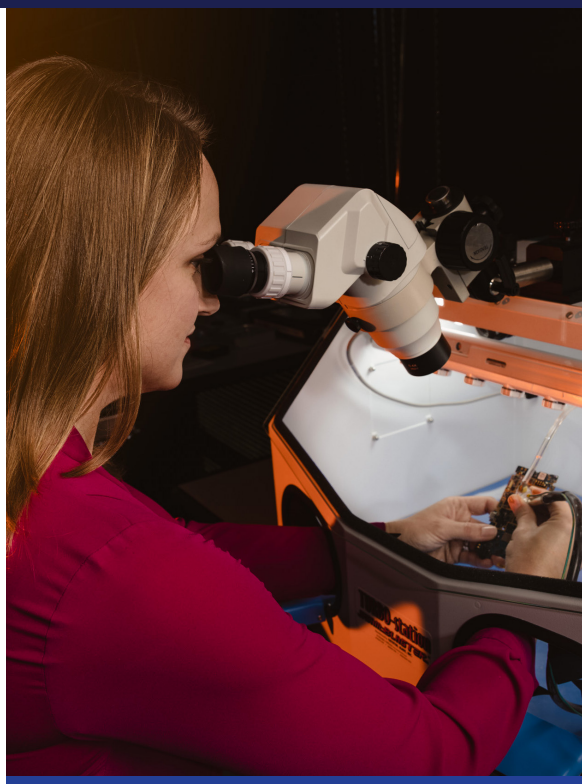
FACT SHEET

DoD CYBER CRIME CENTER (DC3)

The DoD Cyber Crime Center (DC3) was established as an entity within the Department of the Air Force in 1998 and was officially designated a United States Air Force Field Operating Agency by the Secretary of the Air Force, effective Jan. 15, 2021.

DC3 provides digital and multimedia (D/MM) forensics, specialized cyber training, technical solutions development, and cyber analytics for the following DoD mission areas: cybersecurity (CS) and critical infrastructure protection; law enforcement and counterintelligence (LE/CI); and document and media exploitation (DOMEX). In addition, DC3 responds to queries regarding counterterrorism and cyber safety. DC3 delivers superior results by synthesizing its six functional directorates' expertise into a single holistic capability.

DC3 is designated as a Federal Cybersecurity Center by National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and as a DoD Center of Excellence for D/MM forensics by DoD Directive 5505.13E. It serves as the operational focal point for the Defense Industrial Base Cybersecurity Program (DIB CS Program; 32 CFR Part 236). DC3 delivers capabilities with a team comprised of Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized support.



A DC3 lab specialist extracts data from damaged media: one of the most challenging but important services the lab provides.

DC3 hosts embedded liaisons from numerous mission partners, to include DoD LE/CI organizations, the National Security Agency (NSA), U.S. Cyber Command (USCYBERCOM), four distinct Damage Assessment Management Offices (Office of the Secretary of Defense and the three Military Departments), a Joint Acquisition Protection and Exploitation Cell, and an Air Force Life Cycle Management Center element. DC3 also maintains enduring partnerships with the FBI, the National Media Exploitation Center (NMEC), and other core mission partners via embedded DC3 liaisons.

DoD CYBER CRIME CENTER

410-981-6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics DC3 Cyber Crime Center

OPERATIONS

Cyber Forensics Laboratory (CFL)–The CFL conducts D/MM forensic examinations, repairs damaged devices, extracts device data, and provides expert testimony for the DoD. The lab's robust intrusion and malware analysis capability also supports other DC3 lines of effort, and specifically supports DoD LE/CI organizations. CFL recently expanded its capabilities by adding unlock services for mobile devices, and has experienced a 97 percent unlock success rate since launching this service. CFL is the largest DoD D/MM lab and is accredited under ISO 17025 by the ANSI National Accreditation Board (ANAB), which provides strict guidance regarding reliable, repeatable and valid exam procedures subject to quality control and peer review.

Cyber Training Academy (CTA)–The CTA provides classroom and web-based cyber training through more than 30 unique courses to DoD entities that protect DoD information systems from unauthorized, criminal, fraudulent, and foreign intelligence intrusions. The Academy confers DoD certifications in digital forensics and cyber investigations. To complement its in-residence training, CTA offers an extensive distance learning program (https://www.dcita.edu) and maintains formal relationships with 16 institutes of higher learning. During FY21, the CTA delivered a total of 468,755 training hours from in-residence, online, Instructor-Led Virtual (ILV), and Mobile Training Team (MTT) learning offerings to students with duties in DoD LE/CI, Cybersecurity, Intelligence, and Cyber Mission Forces.

Department of Defense-Defense Industrial Base (DoD-DIB) Collaborative Information Sharing Environment (DCISE)–DCISE assists nearly 1,000 companies in a voluntary partnership to understand the risks from nation-state threats, and aids them in elevating their cybersecurity to better safeguard unclassified DoD information residing on or transiting their corporate networks. As the DoD operational hub for this effort, DCISE provides partner companies actionable indicators for their network defense systems (nearly 484,000 so far) and tailored analyses to aid remediation efforts for cyber incidents. Supported by CFL, partner companies have benefited from more than 75,000 hours of no-cost intrusion forensic analysis and malware reverse engineering products and services. To enhance partner cybersecurity expertise, DCISE also delivers face-to-face consults with company cybersecurity (CS) analysts and executives, and conducts interactive group technical exchanges with partner CS experts. DCISE is also the designated DoD repository for all defense contractor cyber incident reporting under DFARS 252.204-7012 requirements. Follow DCISE on Twitter, where its handle is "**@DC3DCISE**".

Operations Enablement Directorate (OED)–OED focuses on amplifying the effects of DoD-wide LE/CI investigations and operations, and by extension, the effects of the U.S. Intelligence Community at large. OED conducts sharply focused technical and cyber intelligence analysis leveraging multiple sources of data and unique analytic tools, applications, and capabilities to directly support stakeholder requirements and priorities. OED also supports joint operations by managing the development, sustainment, and enhancement of operational support systems, while working closely with OUSD(I&S) and the DoD CI community to define and prioritize new technical capability development.

Technical Solutions Development (TSD)–The TSD serves as the technical solutions development capability for DC3. As such, it provides custom-tailored software and IT systems solutions to support digital forensic examiners and cyber intrusion analysts, including providing OED, DCISE, CFL, and VDP with tools and techniques engineered to meet specific requirements. TSD also develops tools, such as DC3 Advanced Carver, which enhance data extraction efforts in response to various DoD requirements, such as DOMEX. TSD conducts test and validation services on both commercial off-the-shelf and government off-the-shelf hardware, as well as in-house-developed software, before its release for use in forensic processes (a prerequisite for lab accreditation).

Vulnerability Disclosure Program (VDP)–The Secretary of Defense directed DC3 to begin VDP operations in November 2016, to better align the DoD with private industry. Supporting the DoD Chief Information Officer (CIO), United States Cyber Command (USCYBERCOM), Joint Force Headquarters DODIN (JFHQ-DODIN), and the cyber elements of all DoD components, VDP crowdsources the expertise of private-sector cyber security researchers to identify vulnerabilities on DoD information systems. As the largest such program in the world, the VDP triages every vulnerability submitted to it, coordinates with system owners for mitigation, and assesses the technical effectiveness of fix actions. The VDP provides an independent assessment of DoDIN security and defensive measures, discovers vulnerabilities not previously found by existing red-teams or automated systems, and proactively identifies noncompliance with technical standards. Follow VDP on Twitter, where its handle is "**@DC3VDP**".