A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

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 January 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 composed of Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized support.

DC3 VISION

Enable insight and action in cyberspace and beyond

DC3 MISSION

A Federal Cyber Center that delivers innovative capabilities and expertise to enable and inform law enforcement, cybersecurity, and national security partners

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 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 20 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. CTA delivers training via 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.

DoD-Defense Industrial Base (DoD-DIB) Collaborative Information Sharing Environment (DCISE)–DCISE assists over 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 and tailored analyses to aid remediation efforts for cyber incidents. 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.

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 the Office of the Under Secretary of Defense for Intelligence & Security and the DoD CI community to define and prioritize new technical capability development.

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.

Strategy and Partner Engagement (XE)–In 2023, DC3 established the Directorate of Strategy and Partner Engagement (XE) by integrating the offices of Public Affairs, Plans and Policy, Organizational Development, and Executive Support Staff. The creation of XE unified elements dedicated within DC3 to providing organizational outreach and strategic engagement across the federal government and internationally. In an effort to increase cross-collaboration and partnership initiatives throughout DC3, XE leaders established reoccurring core functional Mission Enablement Workshops to facilitate continued development of agency cohesion. Session curriculum aims to facilitate full-spectrum awareness of the organization by all employees.

Information Technology (XT)–XT 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. XT also develops tools, such as DC3 Advanced Carver, which enhance data extraction efforts in response to various DoD requirements, such as DOMEX. XT 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).