



DC3

Defense Cyber Crime Center
Air Force Office of Special Investigations

Fact Sheet

Department of the Air Force

MISSION STATEMENT

Deliver superior digital forensics and multimedia lab services, cyber technical training, research, development, testing and evaluation, and cyber analysis capabilities supporting cyber counterintelligence and counterterrorism, criminal investigations, intrusion forensics, law enforcement, intelligence community, critical infrastructure partners, and information operations for the Department of Defense.

DEFENSE CYBER CRIME CENTER (DC3)

DC3 provides digital and multimedia (D/MM) forensics, cyber investigative training, research, development, test and evaluation (RDT&E), and cyber analytics for the following DoD mission areas: information assurance (IA) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT).

DC3 was established as an organic entity within the Air Force Office of Special Investigations in 1998. DC3 is a national cyber center, as recognized in NSPD 54/HSPD 23 and serves as the operational focal point for the Defense Industrial Base Cybersecurity and Information Assurance Program (DIB CS/IA Program).

DC3 is located in Linthicum, MD with a staff of approximately 400, including DoD civilians, military, and contract partners. DC3 also hosts 23 liaisons/detailees from other agencies, including the Department of Homeland Security, OUSD (AT&L) Damage Assessment Management Office (DAMO), National Security Agency, Federal Bureau of Investigation, Defense Criminal Investigative Organizations, U.S. Army Military Intelligence, and U.S. Cyber Command.



DEFENSE CYBER CRIME CENTER

Air Force Office of Special Investigations
410-981-1181 | www.dc3.mil | dc3@dc3.mil



DC3

Defense Cyber Crime Center Air Force Office of Special Investigations



OPERATIONS

DC3's capabilities are delivered via functional organizations, which create synergies and enable considerable capability for its size.

Defense Computer Forensics Laboratory (DCFL). DCFL delivers digital and multimedia (D/MM) evidence processing, forensic examinations, and expert testimony for any DoD Agency requiring D/MM services. The laboratory's robust intrusion and malware capability provides support to other DC3 lines of business and activities hosted at DC3, such as the OUSD (AT&L) DAMO. DCFL operations are accredited for "Forensic Science Testing" under ISO 17025 by the American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB). During FY12, the lab performed 1,406 forensic examinations involving 834.58 terabytes of data.

Defense Cyber Investigations Training Academy (DCITA). DCITA provides classroom and web-based cyber investigative and incident response training via 33 courses and five specialty tracks to DoD elements that protect DoD information systems from unauthorized use and criminal, fraudulent, and foreign intelligence activities. DCITA confers DoD certifications in digital forensics, cyber investigations, and incident response. During FY12, DCITA provided 3,498 units of cyber investigative training. DCITA is also leading the Center for Digital Forensics and Academic Excellence (CDFAE) program. Currently, the program involves eight colleges, universities and institutes of higher learning in an effort to establish a national core curriculum in digital forensics.

Analytical Group (AG). DC3's AG provides cyber analysis products and services to LE/CI agencies to support their investigations and operations; principal among them AFOSI, NCIS, and FBI. As a community partner with the National Cyber Investigative Joint Task Force (NCIJTF-AG), the AG leads a collaborative analytical and technical exchange with subject matter experts from LE/CI, CND, IC, and IA agencies to build a threat picture to enable proactive LE/CI cyber operations focused on nation-state threat actors.

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE). DCISE, pronounced "*dice*," is the operational arm of the DoD Cyber Security / Information Assurance program. DCISE works with DIB partners to safeguard DoD information residing on or transiting DIB controlled unclassified networks by providing actionable threat products, analysis, forensics diagnostics, and remediation consults in response to voluntarily reported network events.

Defense Cyber Crime Institute (DCCI). DCCI is the research, development, test, and evaluation (RDT&E) arm of DC3. DCCI supports the AG, DCISE, and DCFL with tools and techniques tailored to the specific requirements of digital forensic examiners and cyber intrusion analysts. On the test and evaluation side, DCCI validates COTS, GOTS, and in-house developed software / hardware before it can be used in a forensic process (a prerequisite for DCFL accreditation). In addition, DCCI performs certification and accreditation of software for use on DC3's networks. DCCI is the DoD repository for cyber CI tools.

Effective: 1 May 2013