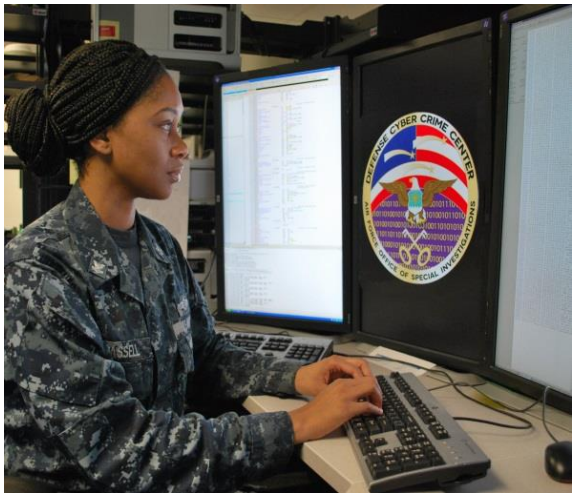
A NATIONAL CYBER CENTER

DC3 Defense Cyber Crime Center
Air Force Office of Special Investigations

Fact Sheet

Department of the Air Force

DEFENSE CYBER CRIME CENTER (DC3)



Established as an entity within the Department of the Air Force in 1998, DC3 provides digital and multimedia (D/MM) forensics, cyber investigative training, technical solutions development, 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 delivers capability via five functional organizations which create synergies and enable considerable capability for its size.

DC3 is designated as a national cyber center by National Security Presidential Directive 54 / Homeland Security Presidential Directive 23, as a DoD center of excellence for D/MM forensics by DoD Directive 5505.13E, and serves as the operational focal point for the Defense Industrial Base Cybersecurity and Information Assurance Program (DIB CS/IA Program; 32 CFR Part 236). DC3 delivers capability with a team of approximately 400 people, comprised of Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized staff support.

DC3 hosts liaisons from numerous mission partners, to include the Department of Homeland Security, the Office of the Under Secretary of Defense for Acquisitions, Technology, and Logistics (OUSD-AT&L) Damage Assessment Management Office (DAMO), National Security Agency, Federal Bureau of Investigation, DoD LE/CI organizations, U.S. Army Military Intelligence, and U.S. Cyber Command.

DEFENSE CYBER CRIME CENTER
Air Force Office of Special Investigations
410-981-6610 | www.dc3.mil | dc3@dc3.mil

Effective: 20 Feb 2015

OPERATIONS

Defense Computer Forensics Laboratory (DCFL) -- DCFL performs D/MM forensic examinations, device repair, data extraction, and expert testimony for DoD. The lab's robust intrusion and malware analysis capability also supports other DC3 lines of business and activities, such as the OUSD (AT&L) DAMO. DCFL operations are accredited under ISO 17025 by the American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB) which guides reliable, repeatable and valid exam results, subjected to quality control and peer review. During FY14, the lab processed 958.28 terabytes of data in 1,202 forensic examinations.

Defense Cyber Investigations Training Academy (DCITA) -- DCITA provides classroom and web-based cyber investigative and incident response training via five specialty tracks and 29 courses to DoD elements that protect DoD information systems from unauthorized, criminal, fraudulent, and foreign intelligence activities. DCITA confers DoD certifications in digital forensics, cyber investigations, and incident response. To complement its in-residence training, DCITA has an extensive distance learning program (see DCITA.edu). During FY14, DCITA filled 6,626 seats in various modes of training.

Analytical Group (AG) -- DC3's AG performs sharply focused technical analyses to support the investigations and operations of LE/CI agencies, principal among them AFOSI, NCIS, and FBI. As a member agency of the National Cyber Investigative Joint Task Force (NCIJTF), the AG also leads collaborative analytical and technical exchanges with subject matter experts from LE/CI, computer network defense (CND), intelligence community (IC), and IA agencies to enable proactive LE/CI cyber operations focused on nation-state threat actors.

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE) -- As the operational hub for the DIB Cybersecurity / Information Assurance Program, DCISE assists DIB companies to safeguard DoD content and intellectual property residing on or transiting their unclassified networks. DCISE develops and shares actionable threat products, and performs cyber analysis, diagnostics, and remediation consults for DIB Partners with DCFL support for malware analysis and intrusion forensics. DCISE is the reporting and analysis center for the implementation of the statutory requirement in Section 941 of the FY2013 National Defense Authorization Act for reporting cyber incidents by Cleared Defense Contractors (CDCs), and the related amendment of the Defense Federal Acquisition Regulations (DFARS), known as "Safeguarding DFARS." DCISE has been appraised at a Maturity Level 3 rating by Carnegie Mellon's Capability Maturity Model Integration for Services. Since FY08, DCISE has shared more than 109,994 intrusion indicators and processed more than 4,839 reports on significant cyber events of concern to DoD and the DIB.

Defense Cyber Crime Institute (DCCI) -- As DC3's technical solutions development capability, DCCI tailors software and system solutions to support the AG, DCISE, and DCFL with tools and techniques engineered 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's ASCLD/LAB accreditation). In addition, DCCI performs certification and accreditation of software for use on DC3's networks and functions as the DoD repository for cyber CI tools.