A FEDERAL CYBER CENTER

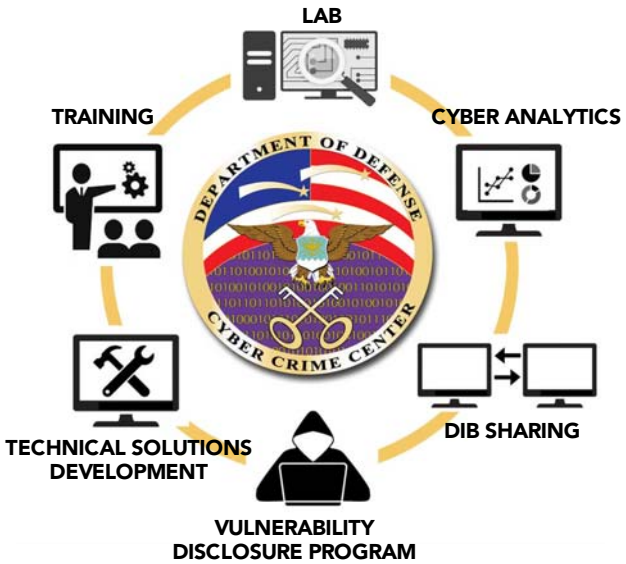
DC3 Department of Defense Cyber Crime Center

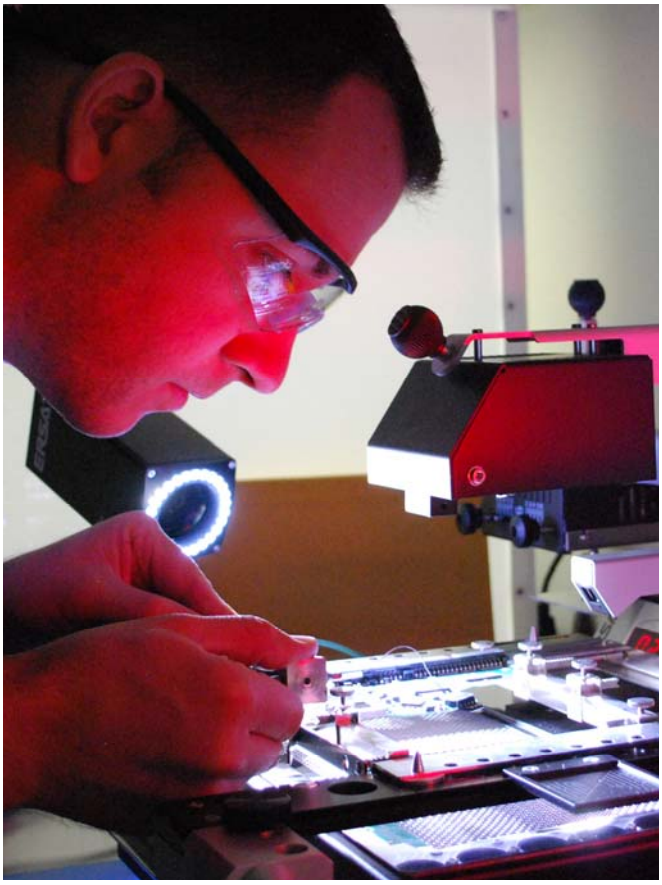
12/15/2017

FACT SHEET
DoD 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, specialized cyber training, technical solutions development, and cyber analytics for the following DoD mission areas: cybersecurity (CS) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT). DC3 delivers capability via six functional organizations which create synergies and enable considerable capability for its size.

DC3 is designated as a federal 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 Program (DIB CS Program; 32 CFR Part 236). DC3 delivers capability with a team of approximately 430 people, 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.

Photo by Al Fiterman

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.

DoD CYBER CRIME CENTER
410-981-6610 | www.dc3.mil | info@dc3.mil

OPERATIONS

Cyber Forensics Laboratory (CFL) -- CFL 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. CFL 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.

Cyber Investigations Training Academy (CITA) -- The academy provides classroom and web-based cyber training via more than 30 courses to DoD elements that protect DoD information systems from unauthorized, criminal, fraudulent, and foreign intelligence activities. The academy confers DoD certifications in digital forensics and cyber investigations. To complement its in-residence training, the academy has an extensive distance learning program (DCITA.edu). During FY17, the academy delivered a combined total of 255,066 hours of training via classroom and online learning to students with duties in DoD Law Enforcement/Counterintelligence, Cybersecurity, Intelligence, and Cyber Mission Forces.

Analytical Group (AG) -- DC3's AG performs sharply focused technical analyses to support the cyber investigations and operations of LE/CI agencies, principal among them AFOSI, NCIS, and FBI. As a member 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, cybersecurity, and the intelligence community (IC), to enable proactive LE/CI cyber operations focused on nation-state threat actors.

Department of Defense-Defense Industrial Base (DoD-DIB) Collaborative Information Sharing Environment (DCISE) -- In a voluntary partnership DCISE assists 480+ companies 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 200K, so far) and tailored analyses to aid remediation efforts for cyber incidents. Supported by DC3's Cyber Forensics Lab, partner companies have benefited from 40K+ hours of no-cost intrusion forensics and malware reverse engineering. To enhance partner cybersecurity expertise DCISE also delivers face-to-face consults in 1-to-1 discussions with company cybersecurity analysts, or company cybersecurity executives, and conducts interactive group technical exchanges (TechEx's) with partner cybersecurity experts. DC3/DCISE is also the designated DoD repository for all defense contractor reporting under DFARS 252.240-7012 requirements.

Technical Solutions Development (TSD) -- As DC3's technical solutions development capability, TSD tailors software and system solutions to support digital forensic examiners and cyber intrusion analysts, including AG, DCISE, and CFL, with tools and techniques engineered to their specific requirements. TSD also develops tools such as DC3 Advanced Carver to aid data extraction for various DoD requirements such as DOMEX. On the test and evaluation side, TSD validates commercial off-the-shelf (COTS), government off-the-shelf (GOTS), hardware and in-house developed software before use in a forensic process (a prerequisite for lab accreditation).

Vulnerability Disclosure Program (VDP) -- The Secretary of Defense directed DC3 to begin VDP operation in 2016. Supporting the DoD Chief Information Officer, U.S. Cyber Command, Joint Force HQs – DoDIN, and the cyber elements of all DoD components, the VDP crowdsources the expertise of private-sector cyber security researchers to identify vulnerabilities on DoD information systems. DC3/VDP evaluates reported vulnerabilities, forwards valid vulnerabilities for mitigation, and validates the effectiveness of mitigation actions to provide an independent assessment of DoDIN security and defensive measures, discover vulnerabilities not found by existing red-team and automated efforts, and identify compliance and training deficiencies. The result is improved DoD network defense and mission assurance.