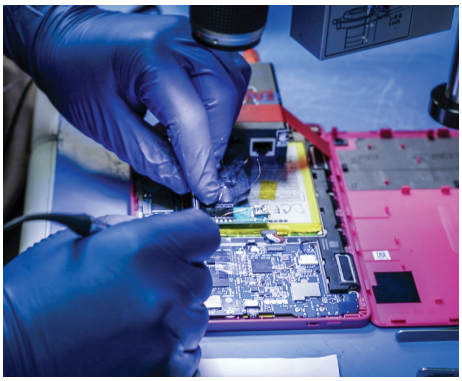
DoD CYBER CRIME CENTER

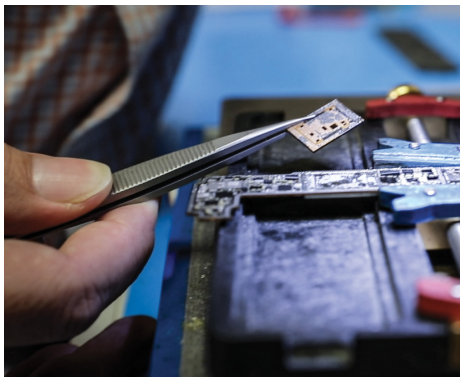
A FEDERAL CYBER CENTER

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 Department of the Air Force, effective January 15, 2021.

DC3 provides digital and multimedia forensics, specialized cyber training, technical solutions development, and cyber analytics for the following DoW mission areas: cybersecurity and critical infrastructure protection, law enforcement and counterintelligence, and document and media exploitation. In addition, DC3 responds to queries regarding counterterrorism and cyber incident. DC3 delivers superior results by synthesizing its functional directorates' expertise into a single holistic capability.

DC3 is designated as a Federal Cyber Center by National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and as a DoW Center of Excellence for digital and multimedia forensics by DoD Directive 5505.13E. It serves as the operational focal point for the Defense Industrial Base Cybersecurity Program (DoW CIO). DC3 delivers capabilities with a team composed of Department of the Air Force civilians, military, and specialized contractor personnel.





Primary Lines of Effort

- Expert digital and multimedia forensic capabilities to support military investigations and operations
- Rapid development and delivery of cyber training for U.S. and international partners
- Target packages and finished intelligence analysis of cyber threats to enable insights and action
- Cybersecurity protection of global supply chains, defense acquisitions, and critical infrastructure
- Vulnerability disclosure partnership with U.S. Cyber Command

DC3 MISSION

DC3 empowers action in cyberspace through innovation, collaboration, and world-class training to reduce cyber risks and build a secure future

DC3 VISION

Enable insight and action in cyberspace and beyond

Pub. Date 25 FEB 2026

OPERATIONAL DIRECTORATES

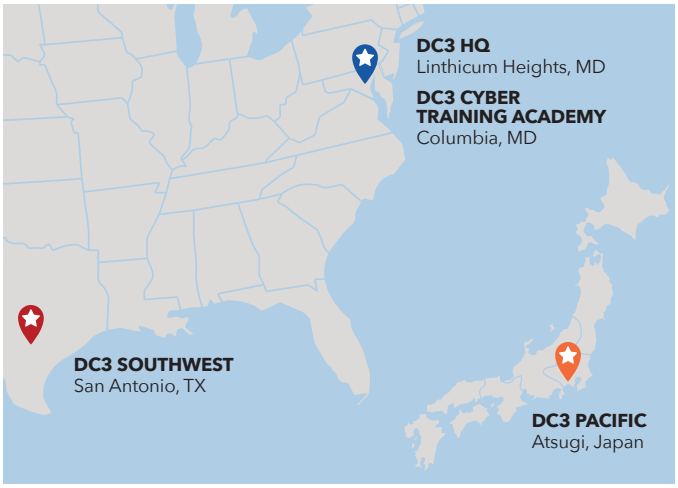
Cyber Forensics Laboratory (CFL)
CFL operates a state-of-the-art facility, using leading-edge technology and its technically diverse talent pool to provide timely, innovative processing and analysis of digital evidence for DoW investigations. CFL performs digital and multimedia forensic examinations, device repair, data extraction, and expert testimony for the DoW.

Cyber Training Academy (CTA)
CTA designs, develops, and delivers the highest quality cyber training to DoW operators, U.S. Government personnel, and allied partners whose duties include ensuring defense information systems are secure from unauthorized use, counterintelligence, and criminal and fraudulent activities.

DoD-DIB Collaborative Information Sharing Environment (DCISE)
As the operational hub for the DoW's Defense Industrial Base (DIB) CS Program, DCISE assists DIB companies in safeguarding unclassified DoW information and intellectual property residing on or transiting through unclassified networks. DCISE develops and shares actionable threat products and performs cyber analysis, diagnostics, and remediation consults for industry partners.

Information Technology (XT)
XT manages a vast array of IT operating systems and provides technical solutions to support both the DoW intelligence and law enforcement communities. XT also functions as the DoW repository for cyber counterintelligence tools.

DC3 OPERATING LOCATIONS



Operational Enablement Directorate (OED)
OED is focused on amplifying the effects of DoW-wide law enforcement and counterintelligence investigations and operations, and by extension, the effects of the U.S. Intelligence Community at large. OED consists of two teams: The Analytical Group (OED/AG) and the Special Capabilities Group (OED/SCG).

Vulnerability Disclosure Program (VDP)
VDP operates the DoW's Vulnerability Disclosure Program, which leverages the global ethical researcher community to identify cyber-based vulnerabilities and harden critical infrastructure control systems, weapons systems, mobile applications, and Internet of Things within the DoW information networks.