2025

DoD CYBER CRIME CENTER

ANNUAL REPORT

A FEDERAL CYBER CENTER

DC3 MISSION

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

DC3 VISION

Enable insight and action in cyberspace and beyond

DIRECTOR'S MESSAGE

Welcome to the 2025 Department of Defense Cyber Crime Center (DC3) Annual Report.

Established within the Department of the Air Force (DAF) in 1998, for nearly three decades DC3 has been entrusted with numerous missions critical to ensuring national security. As a Federal Cyber Center, DC3 delivers superior digital and multimedia forensics services, cyber technical training, vulnerability sharing, technical solutions development, and cyber analysis within the Department of War mission areas: cybersecurity and critical infrastructure protection, law enforcement and counterintelligence, documents and media exploitation, and counterterrorism.

Our focus remains on developing cutting-edge solutions and results that exceed our customers' expectations. Our talented workforce is leading the edge of purposeful innovation—aiding critical partners in their ability to outpace our adversaries.

From our initial charter, our responsibilities and capabilities have grown substantially. Our evolution from a specialized laboratory into a multi-faceted Center of Excellence is a testament to the adaptability and expertise that define this organization.

I am honored to lead this exceptional organization and welcome you to explore the accomplishments, celebrations, and organizational milestones highlighted within this 2025 Annual Report.

One Team, One Mission

Lesley H. Bernys

Special Agent Lesley H. Bernys
DC3 Executive Director

DIB CYBERSECURITY

DoW-DIB Collaborative Information Sharing Environment (DCISE)

DCISE operationally supports the DoW Chief Information Officer (CIO) as the single focal point for receiving all cyber incident reports affecting unclassified contractor networks and Controlled Unclassified Information (CUI), or a contractor's ability to provide Operationally Critical Support, in accordance with (IAW) the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012.

CY25 Yielded

170,503

Actionable IOCs

1,296

Cyber Threat Reporting Products

MISSION HIGHLIGHTS

DCISE Develops Malware Information Sharing Platform (MISP)

To enable the rapid, automated sharing of Cyber Threat Information (CTI) with DIB Partners and other government agencies, DCISE began development of a MISP instance to improve the speed and scale of CTI dissemination. This platform is one of the most widely adopted methods for automated threat sharing and will significantly enhance collaboration between DC3, the DIB, and other domestic and foreign partners.

DCISE Threat Information Sharing Efforts Enhanced

DCISE conducted 26 combined Analyst-to-Analyst (A2A) meetings and Focused Analytical Outreach sessions with individual DIB Partners. DCISE conducted 14 briefings for organizations such as the Joint Counterintelligence Training Academy (JCITA) and Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

CYBER FORENSICS

Cyber Forensics Laboratory (CFL)

CFL operates an accredited 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 D/MM forensic examinations, device repair, data extraction, and expert testimony for the DoW.

FORENSICS HIGHLIGHTS

Trial counsel notified CFL that a defendant involved in a case requiring DC3 forensics analysis had pled guilty to rape of a child under age 12 and producing and possessing Child Sexual Abuse Material (CSAM). The defendant received a 40-year sentence and a dishonorable discharge.

A malware reverse engineer attributed a malicious file that collects multiple browser activity data points including user tracking to a nation-state actor. The file contained both a previously known C2 domain and a newly identified domain.

Damaged media recovery experts reconstructed and extracted data from a failing server. Using specialized tools and subject matter expertise, the technicians quickly reconstructed two RAID 5 storage servers and recovered 33TB of data.

While operating from DC3 Headquarters in Maryland, a cryptography SME performed CFL's first remote retrieval of a BitLocker recovery key for an encrypted drive associated with a CSAM exam being conducted at CFL Southwest - Operating Location.

Completed
855
Digital Forensic Exams

2,012
Evidence Items

2,112 TBs
of Data

322
Exams Completed Involving Systems and Malware Intrusions

28%
of these Exams Involved Crimes Against Children

MISSION HIGHLIGHTS

DC3 Foreign Special Project Support

Throughout 2025, DC3 facilitated the establishment of numerous foreign liaison projects to aide in advancing capabilities throughout Europe, the Indo-Pacific, and Middle East in partnership with AFOSI and NCIS. Project Hermione was initiated in support of French law enforcement and cyber organizations, DC3 Pacific was brought to full operating capabilities to support the Indo-Pacific region, and Project Khanjar to support Oman. Support includes expansion of cyber threat information sharing and subject matter analytical exchanges.

Release of CFL Electronic Request Form (CERF) Application

CERF is a web application allowing customers to request an intrusions examination by CFL. XT released version 1.1 of this application, which allows users to electronically complete CFL's Form 1 to request intrusions exams.

CYBER TRAINING

Cyber Training Academy (CTA)
CTA provides students with the skills needed to meet mission goals in the cyber environment. Our Academy's training prepares DoW personnel in cyber-force specialty areas with the knowledge and expertise to utilize various tools and techniques to investigate, audit, defend, monitor, detect, analyze, and mitigate threats to DoW networks and information technology systems. The curriculum focuses on forensics, technologies, intelligence, and tools, and trains students in areas such as:

- Digital media examination on multiple operating system platforms in a lab environment or a deployed setting
- Network intrusion basics and log analysis
- Successfully installing software to assess network vulnerabilities
- Collecting and analyzing digital evidence, spanning varying levels of operational and technical complexity
- First-response fundamentals, basic cyber investigative practices and tools and cyber investigation unit management

CTA Council on Occupational Education (COE) Accreditation
COE grants accreditation to career and technical education institutions that demonstrate quality, integrity, and student achievement. Achieving accreditation with COE is a nationally recognized mark of excellence and proves an occupational education institution's credibility. CTA hosted a 3-member visiting team for a COE Reaffirmation Site Visit who confirmed CTA compliance with COE's 10 standards as outlined in the Accreditation Handbook. COE granted CTA reaccreditation for a continuing 6 years.

CTA Drone Forensics Course Development
CTA successfully completed development of a Drone Forensics course designed to provide comprehensive instruction on the collection, examination, and analysis of forensics artifacts associated with Unmanned Aerial Systems (UAS) and related peripherals.

248,540
Training Hours Delivered

9,676
Total CyberCasts

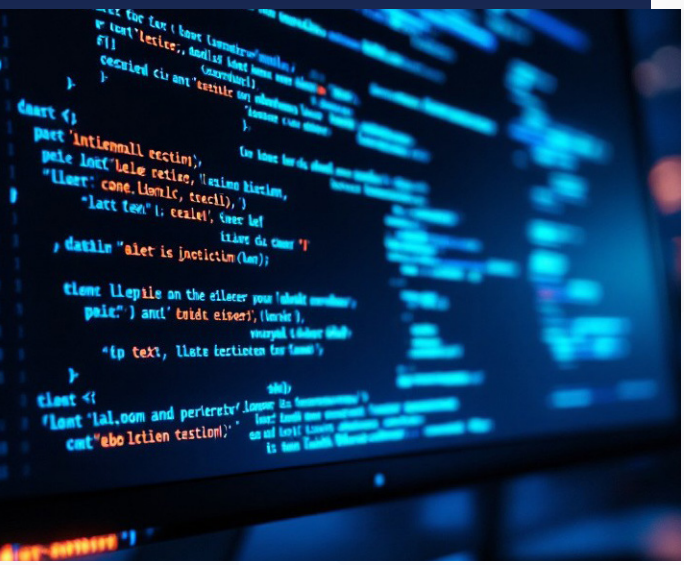
560
Hours of Training to Foreign Partners

32,574
Hours of On-demand Training

INFORMATION TECHNOLOGY

Directorate of Information Technology (XT)

XT provides technical solutions and systems expertise for the DC3 mission spaces as well as external stakeholders providing tools and services to DoW National Security partners and Law Enforcement communities. XT functions as the DoW repository for cyber counterintelligence tools. Staff expertise includes help desk, technical, and project support, as well as creating innovative solutions, enterprise architecture, records management, and knowledge management. XT is responsible for modernizing legacy information architectures, securing data collection assets to enable partnerships, and enabling mission-relevant machine learning and artificial intelligence capability fielding.



MAJOR PROJECTS

AFNET Transition

DC3 CIO made significant progress in transitioning DC3's NIPR and SIPR implementations from on-premise infrastructure (DEN and SDEN) to AF-hosted cloud-based solutions (AFNET and AFNET/S). This transition will allow DC3 to be more closely integrated with Air Force systems and receive services provided through AFNET and AFNET/S which would otherwise be unavailable. Transition to AFNET is scheduled to be completed by September 2026.

Cloud Migration

XT continued efforts to migrate applications from traditional on-premises to DAF cloud environments (DAF CLOUDworks and CloudOne.) Currently, DC3 has prepared existing applications to support migration to and running within a DAF.

DevSecOps Implementation

XT has successfully integrated DevSecOps procedures and automated pipelines across select projects, marking a critical shift toward agile, secure software delivery. By embedding security protocols directly into the development lifecycle, XT ensures that mission-critical capabilities are deployed to end-users with increased velocity, without compromising the rigorous security posture required for operational success.

OPERATIONS ENABLEMENT

Operations Enablement Directorate (OED)
OED is focused on amplifying the effects of DoW-wide Law Enforcement and Counterintelligence (LE/CI) 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).

Published
882
Cyber Products

Published
88
Joint Interagency Cyber Reports

188
Products Cited in IC Reports

MISSION HIGHLIGHTS

Combating Cryptocurrency Ransomware
OED analysts enabled law enforcement partners to arrest high-profile cybercriminals and/or freeze cryptocurrency accounts linked to cybercriminal groups to include ransomware, disrupting the groups' ecosystems and cyber operations. OED analysts traced $18.7 billion in digital assets since July 2023.

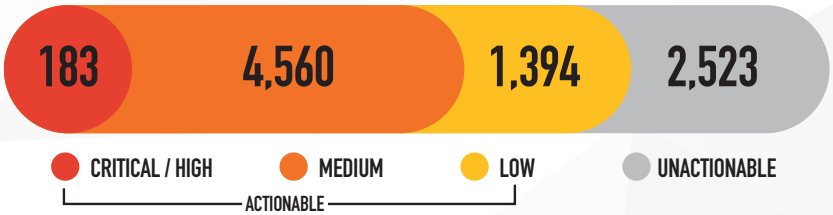
DC3 Cyber Partnership with NAVSEA and U.S. Coast Guard
OED AG hosted a Technical Exchange Meeting with the Naval Sea Systems Command (NAVSEA), the largest of the United States Navy's five systems commands, or materiel organizations. The United States Coast Guard (USCG) Cyber Command attended the meeting to address ongoing cyber issues at U.S. Navy shipyards and facilities supporting Navy contracts. A collaboration portal was created with a goal to identify new collaborative opportunities to mitigate or resolve significant maritime cyber threats to protect U.S. critical infrastructure and national security.

VULNERABILITY DISCLOSURE

Vulnerability Disclosure Program (VDP)

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

SEVERITY FOR CY25



MISSION HIGHLIGHTS

Rapid VDP Response Campaigns

Vulnerability assessments prompted by active and live exploits observed in open-source environments. During research, analysts highlight active exploits based on notifications or trends and then search for affected assets. Initial campaign kickoff was initiated by the 2025 exploit of a VMware vulnerability.

VDP HACKER-POWERED SECURITY

58,436
Vulnerabilities
(since launch)

5,479
Researchers
(since launch)

4,456
New Vulnerabilities
(in 2025)

DIB-VDP Onboarding Automations

DIB-VDP automations are features implemented within the DIB Vulnerability Report Management Network (VRMN) platform to allow for streamlined customer onboarding. The automations include bulk asset file uploads and an automated Terms of Service agreement.

Hack the Pentagon

To continue running DoW Bug Bounty campaigns after the dissolvement of Defense Digital Services (DDS), responsibilities of Hack the Pentagon (HtP) were transferred to DC3's VDP. HtP had been running since 2016 and is the origin of the enduring VDP program. DC3 has developed a Bullet Background Paper for HtP funding and submitted for the FY28 POM cycle.

DIB-VDP HACKER-POWERED SECURITY

976
Vulnerabilities
(since launch)

128
Actionable Reports

39
Successfully Mitigated
(to date)

ENTERPRISE MANAGEMENT

Enterprise Management and Resources (ER)
ER provides effective and efficient management of DoW and DAF resources that are linked to the DC3 functional mission, strategic planning, programming, budgeting, and performance reporting; and serves as the agency's focal point for requirements management and associated processes.

Maj. Gen. Daniel DeVoe
Commander of the Air Force District of Washington

MISSION HIGHLIGHTS

Requirements, Prioritization & Investment Board (RPIB)
The RPIB process was redesigned to collect, manage, and prioritize new unfunded internal/external requirements across the DC3 Enterprise. This resulted in effective enterprise management of new unfunded requirements.

Joint Knowledge Online (JKO) Dashboard Tracking
DC3's Senior Enlisted Leader developed a weekly dashboard for DC3 Executive Director which depicts training compliancy statistics for each Directorate. Downloaded data capabilities provide monthly JKO compliance reports for 12 respective program managers. Efforts results in an average DC3 JKO compliancy rate of 98.6%.

STRATEGY AND PARTNER ENGAGEMENT

Strategy and Partner Engagement (XE)
XE is composed of elements representing the offices of partner engagement, organizational development, public affairs, and planning and policy. These unified elements provide organizational outreach and strategic engagement across the federal government, international partners, and public sectors.

MISSION HIGHLIGHTS

DC3 Public Affairs (XEC) Outreach Efforts
In an effort to advance mission and strategic lines of efforts, XEC conducted traditional media engagement, speaking engagement coordination, public education series, social media outreach, and videography and graphic design material development. Some of the major initiatives involved keynote speeches supporting Defense Strategic Institute, cyber panels supporting the Scoop News Group, joint fireside interviews supporting DAFITC, radio and podcast interviews supporting Federal News Network, and feature-length film development in support of the International Association of Chiefs of Police and American Academy of Forensics Sciences.

20 Strategic Engagements

23 Media Engagements

29 Executed Agreements

DC3 Adaption of Enterprise Task Management Software Solution (ETMS2)
XE launched DC3's own instance of ETMS2, resolving a year-long effort to implement a viable task management staffing process that could be used to staff external taskers internally to DC3 Action Officers (AO). This reduced the XE manpower requirement by half and has the added advantage of electronic record management exclusive to DC3. XE also launched the first ever DC3 instance of ETMS2 on SIPR.

Pub. Date 07 MAY 2026

DoD CYBER CRIME CENTER

410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

DC3 Cyber Crime Center @DC3Forensics