



DEPARTMENT  
OF DEFENSE  
CYBER CRIME  
CENTER

# ANNUAL REPORT



## 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 2024 Department of Defense (DoD) Cyber Crime Center (DC3) Annual Report.

Established in 1998 as a joint DoD Computer Forensics Laboratory and Cyber Training Program, our history is rooted in developing exquisite capabilities and world class offerings—denoted in our recognition as both a Federal Cyber Center and Center of Excellence for Digital and Multimedia Forensics.

Our organizational vision is to *enable insight and action in cyberspace and beyond*, fostered through a culture of innovation and service. DC3 strives to deliver integrated and advanced capabilities and enhanced insights to our military, law enforcement, cybersecurity, allied, and national security partners both domestically and internationally.

During 2024, DC3 grew to global expansion bringing capabilities across the U.S. and within the Indo-Pacific region. We reaffirmed our commitment to deliver notable results, unparalleled expertise, and expansive support to strategic partnerships worldwide. We sought to streamline our organization and foster a more integrated and resilient team.

With special recognition of our workforce and partners, we invite you to review this 2024 DC3 Annual Report.


Very respectfully,

**LESLEY BERNYS**

Executive Director



# CYBER FORENSICS

 **Cyber Forensics Laboratory (CFL)**  
CFL operates a state-of-the-art facility, using leading-edge technology and a technically advanced talent pool to provide timely, innovative processing and analysis of digital evidence for DoD investigations. CFL performs Digital and Multimedia (D/MM) forensic examinations, device repair, data extraction, and expert testimony for the DoD.

## MISSION HIGHLIGHTS

**DC3-Pacific**  
Due to the proliferation of D/MM devices in the Indo-Pacific Command region, the forensic analysis demand of Military Criminal Investigative Organization (MCIO) and Military Department Counterintelligence Organization (MDCO) has rapidly increased in volume. By leveraging existing U.S. Naval Criminal Investigative Service (NCIS) facilities in Atsugi, Japan, DC3 has addressed the requirement for additional support by initially establishing an INDO-PACOM CFL as an extension of DC3 CFL headquartered in Linthicum, Maryland.

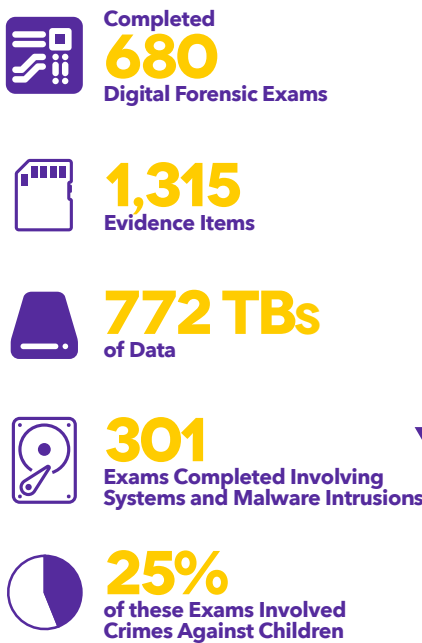
**Deployment of Forensic Advisory Services Team (FAST) 2.0**  
To identify and complete exams that can be closed quickly while providing constant communications.

**DC3 Support to Expert Witness Testimony Training**  
DC3 Judge Advocate and liaisons supported development/execution of Digital Forensics Evidence (DFE) prosecutor course and development of requirements for digital evidence field collections/advocacy course. Provided key support to establishing requirements for digital evidence UCMJ prosecutor training and provided significant input to the awarded developer, National White Collar Crime Center, regarding course content.

## FORENSIC HIGHLIGHTS

A DC3 CFL technician was able to repair a severely damaged iPhone and acquired 100% of the user's data, which led to assistance in a previously stalled investigation.

Due to an examiner's efforts, trial counsel notified CFL that the accused in a child sexual assault case received thirty months' confinement, dishonorable discharge, reduction in grade, total forfeiture of assets, and requirement to register as a sex offender.



The Automated Malware Response (AMR) application has exceeded 5,000 submissions in FY24, an all-time annual high.

# DIB CYBERSECURITY

 **DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)**  
As the operational hub for the DoD's DIB Cybersecurity (CS) Program, DCISE assists DIB companies in safeguarding unclassified DoD 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 DIB partners.

**DCISE Support to F5 Big IP/Volt Typhoon**  
On 19 January 2024, DCISE issued an alert with critical Indicators of Compromise (IOCs) related to Volt Typhoon targeting the DoD. DCISE proactively released the alert one day before widespread Common Vulnerabilities and Exposures was published. DCISE continued to update the alert with new IOCs from U.S. Government (USG) sources, providing timely intelligence to DIB companies. Through active coordination with DC3 and other USG entities, DCISE facilitated the sharing of vital threat information, enhancing collective cybersecurity efforts.

**DCISE Expansion of Adversary Emulation Assessments**  
CY2024 was the first full year that Adversary Emulation Testing (AET) was provided as an enduring capability. Providing AETs helped drive Cyber Resilience Assessments (CRAs) up for the year, resulting in **12 CRAs**. These two activities have provided insights into the DIB that previous DoD organizations have not been able to replicate. As Cybersecurity Maturity Model Certification (CMMC) becomes a reality for the DIB, these services will also help prepare DIB partners for CMMC certifications, and help DC3 identify common vulnerabilities across the DIB.

DCISE integrated Big Data Platform (BDP) for DCISE<sup>3</sup>—providing additional data life and analytical tools for DCISE<sup>3</sup> data.





## CYBER TRAINING



### Cyber Training Academy (CTA)

CTA designs, develops, and delivers high quality cyber training to DoD individuals whose duties include

ensuring defense information systems are secure from unauthorized use, counterintelligence, and criminal fraudulent activities.

### 2024 Course Development Enhancements:

- Dark Web Activities (DWA)
- Online Undercover Activities (OUA)
- Managed Attribution (MA)
- Mac Forensics (MACF)
- Cryptocurrency Activities (CCA)
- Basic/Intermediate/Advanced Malware Analysis (BMA) (IMA) (AMA)



**356,120**

Training Hours Delivered



**7,592**

Total CyberCasts



**1,800**

Hours of Training to Foreign Partners



**2,168**

Hours of On-demand Training



**9,213**

Hours of Mobile Training Teams (MTT) Deployment

## INFORMATION TECHNOLOGY



### Directorate of Information Technology (XT)

In 2023, DC3 established XT, which is composed of the

Architecture Management and Solution Management Divisions. The creation of XT unified IT operations end-to-end and provides the organization with a singular area of focus for IT-related issues, including application development, knowledge management, records management, service desk, network, and software and hardware management.

XT provides technical solutions and network and systems expertise for the DC3 mission spaces as well as external stakeholders providing tools and services to DoD Intelligence and Law Enforcement (LE) communities. XT also functions as the DoD repository for cyber counterintelligence tools. The expertise of the staff involves help desk, technical, and project support as well as creating innovative solutions, enterprise architecture, records management and knowledge management. DC3 manages a variety of specialized networks in support of Defense Criminal Investigations.

## MAJOR PROJECTS

### Implementation of Development, Security, and Operations (DevSecOps)

XT enhances research, development, and deployment of software and systems solutions by integrating DevSecOps principles, which embed security practices throughout the software and systems development lifecycle. DevSecOps facilitates rapid innovation by addressing security concerns iteratively, resulting in higher-quality software and systems while efficiently reducing risk of exploitation.

### DC3's Case Information Management System (CIMS)

CIMS is a business process automation platform designed and utilized by DC3 to enhance the tracking, management, and optimization of digital forensic examinations within CFL. The software has undergone four strategic updates to accommodate DC3's growing forensic lab operations in San Antonio, Texas and Atsugi, Japan, while seamlessly adapting to streamlined workflow enhancements.

### DC3 Data Fusion Suite (DFS)

In coordination with OED/SCG, XT developed DFS with its primary function as providing a platform that integrates and enhances cyber; counterintelligence (CI), defense, and intelligence data across the DoD; acquisitions and technology protection, and DoD and DIB network defense. DFS will provide registered users with secure access to analytic capabilities and intelligence resources in a collaborative environment.



# OPERATIONS ENABLEMENT



## Operations Enablement Directorate (OED)

OED integrates and contextualizes capabilities and data sources across DC3 to illuminate unique cyber risks and opportunities for USG partners. The directorate consists of two teams: the Analytical Group (OED/AG) and the Special Capabilities Group (OED/SCG).

OED/AG conducts highly technical, language-enabled cyber threat analysis leveraging multiple sources of data, unique tools, applications, and capabilities to support stakeholder investigations, operations, and analytic efforts. OED/SCG develops and fields innovative, cross-cutting capabilities to support DC3’s mission partners.



Published  
**592**  
Cyber Products



Attended  
**597**  
Engagements



Finished  
**311**  
IC Citations



## MISSION HIGHLIGHTS

In 2024, the **OED/AG** cryptocurrency team successfully traced over \$1.5 billion in ransoms, and expanded their LE partnerships to 18+ field offices.

**OED/AG** analysts briefed nation-state cyber activity at numerous events including the 2024 Sydney Conference and NATO Cyber Threat Intelligence Conference. Analysts briefed over 540 financial sector attendees on the threat posed by LockBit ransomware groups during a U.S. Department of Treasury conference. OED leadership provided new intelligence on nation-state cyber operations at the U.S. Department of State Trilateral conference co-hosted by Korean and Japanese partners.

**OED/AG** analysts supported significant LE efforts in 2024 to include providing key evidence to support the Department of Justice extradition of a Russian national involved in Phobos ransomware operations—attributed to eight ransomware incidents since 2019. The Russian national and his affiliates extorted more than \$16 million in ransom payments from large corporations, schools, hospitals, and nonprofits.

**OED/AG** facilitated a 10% increase in products disseminated to foreign partners in the U.S. European Command and Indo-Pacific regions.

**OED/SCG** launched the Enhanced Network Sensor and Intelligent Threat Enumeration (ENSITE) Program. Offering near real-time threat intelligence and continuous monitoring via AI/ML capabilities of malicious cyber activity targeting the DIB.

# VULNERABILITY DISCLOSURE

## Vulnerability Disclosure Program (VDP)

DC3 operates the DoD’s VDP, which leverages global crowd-sourced ethical hackers to report vulnerabilities and all publically accessible information systems within the Department of Defense Information Network (DODIN), to include critical infrastructure control, weapon systems, network endpoints, Internet of Things (IoT), and mobile / web applications.



## HACKER-POWERED SECURITY



**53,872**  
Vulnerabilities  
(since launch)



**6,984**  
Researchers  
(since launch)



**4,550**  
New Vulnerabilities  
(in 2024)

## MISSION HIGHLIGHTS

The **Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP)**, launched in June 2024, and is making significant strides. Derived from the major success of the enduring DoD VDP initiative, DIB-VDP brings those same ethical-hackers and crowd-sourcing cybersecurity efforts across the DIB.

**723**

Vulnerabilities  
(since launch)

**301**

Actionable Reports

**108**

Successfully Mitigated  
(to date)

Efforts have protected the DIB from potentially catastrophic data losses, saving the DIB approximately **\$475 billion** in potential costs.

## VDP Integrated Xpanse Project

DC3 facilitated the build out of a capability to host and process Department of Defense Cyber Defense Command (DCDC) Xpanse Attack Surface Management (ASM) alerts. This project was in support of DCDC to establish a common hosting platform for alerts. The capability to process VDP vulnerability reports and Xpanse alerts within the same reporting platform provided DCDC analysts with a single pane of glass for all vulnerability report processing, dissemination, and action.



# ENTERPRISE MANAGEMENT



**Enterprise Management and Resources Directorate (ER)**  
ER provides effective, efficient management of DoD/Air Force resources that are linked to strategic planning, budgeting, and performance reporting and serves as the agency's focal point for contract, logistics, financial, program and requirements management and associated processes and controls.

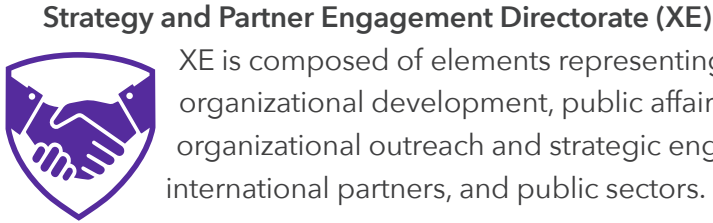
## Law Enforcement Evidence & Data Repository (LEEDR) Development

ER was tasked in April 2024 to chair a DC3 Cross Directorate team to address the need for a study team that would conduct activities to derive requirements to modernize a DoD infrastructure to lawfully store items and data of evidentiary value to MCIO operations to meet current and anticipated mission needs within compliance with policy and law.

In cooperation with MITRE Corporation, DC3 has been working to produce a Capabilities-Based Assessment (CBA) for the Defense Forensic Evidence Networked Data Repository (DEFNDR) which is a subcomponent of the LEEDR.



# STRATEGY AND PARTNER ENGAGEMENT



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



## Support to Office of the National Cyber Director (ONCD) review of Federal Cyber Centers and development of Federal Cyber Center Taxonomy

DC3's Plans and Policy Division (XEX) and directorate personnel met with representatives from ONCD to accurately align DC3 within the new taxonomy and services we provide as an analytical center.

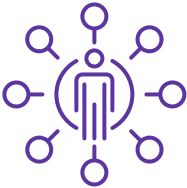
## DC3 Support to rewrite of National Cyber Incident Response Plan (NCIRP)

XEX and other DC3 representatives participated in the Core Planning Team (CPT) for the rewrite of the NCIRP led by Cybersecurity and Infrastructure Security Agency (CISA).

## Support to White House Counter Ransomware Initiative (CRI)

DC3 was honored to host a multi-national delegation from the 4th International CRI, where top leaders joined efforts to combat ransomware on a global scale.

**26**  
Major Media Engagements



**49**  
Foreign/Domestic Engagements





## **DoD CYBER CRIME CENTER**

410.981.6610 | [www.dc3.mil](http://www.dc3.mil)

[DC3.Information@us.af.mil](mailto:DC3.Information@us.af.mil)

✕ @DC3Forensics

in DC3 Cyber Crime Center

Pub. Date JUNE 2025