DEPARTMENT OF DEFENSE
CYBER CRIME CENTER

ANNUAL REPORT 2023

2023

DOD CYBER CRIME 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 2023 Department of Defense (DoD) Cyber Crime Center (DC3) Annual Report.

2023 marked a quarter century of DC3 operations. What began as a joint DoD Computer Forensics Laboratory and Training Program in 1998 has since grown into a Federal Cyber Center and Center of Excellence for digital and multimedia forensics with more than 500 team members.

Building on this history of innovation, DC3 recently published its 2023–2025 Strategic Plan, informed by national and Department of Defense strategic guidance, an informed understanding of challenges and opportunities across the global cyber domain, and input from key stakeholders and partners.

Our organizational vision is to ***enable insight and action in cyberspace and beyond***, which we strive to achieve by fostering a culture of trust and service. DC3 endeavors to deliver innovative capabilities, insights and expertise to law enforcement, cybersecurity, and national security partners globally.

During 2023, DC3 continued to deliver notable results, as summarized in this annual report. In parallel, we streamlined our internal structures and processes, built a more integrated and resilient team, and strengthened our partnerships globally.

With special recognition of our workforce and partners, we invite you to review this 2023 DC3 Annual Report. We welcome your suggestions for the future.

Very respectfully,

JUDE SUNDERBRUCH, SES, DAF
Executive Director
DoD Cyber Crime Center (DC3)

DC3 ENTERPRISE SNAPSHOT

Throughout 2023, DC3 streamlined its organizational structure as a catalyst in our ability to deliver flexible and nimble capabilities to support partner initiatives. DC3 strives to develop a more diverse, equitable, and inclusive workforce whose composition reflects that of our great nation. Moving forward, DC3 will continue to boldly transform the way we operate to meet the evolving needs of our customers and our national security.

Aligned to our 2023–2025 Strategic Plan, we reinvigorated efforts to enrich our engagements with both domestic stakeholders and international partners. Throughout the year, members of the DC3 team represented Department of Defense and U.S. equities abroad in support of U.S. Combatant Command and NATO events and initiatives. In efforts to reach the globally dispersed cyber community, our team welcomed invitations and opportunities to engage more holistically with academic institutions.

Informed by long-standing requirements and the 2022 National Defense Strategy's focus on the Indo-Pacific, DC3 leadership initiated operational endeavors to establish a future operating capability within that region. This DC3 outfit will support DoD investigators and a range of international partners with a compliment of DC3 capabilities.

DC3 CELEBRATES 25TH ANNIVERSARY

In September, DC3 celebrated 25 years of operations with a ceremony held at our headquarters in Linthicum Heights, Maryland. DC3 welcomed more than 300 senior leaders and technical experts from across the United States Government, national and international partners, as well as current and former employees. Distinguished guests from across the DoD and Intelligence Community included leaders from the office of the INTERPOL, Office of the Director of National Intelligence, Office of the National Cyber Director, United States Air Force, U.S. Coast Guard, DoD Chief Information Officer, U.S. Department of Health and Human Services, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, U.S. Cyber Command, Air Force Office of Special Investigations, Army Criminal Investigation Division, Naval Criminal Investigative Service, and many more.

Mr. John Dixson, Director of Defense Intelligence, Counterintelligence, Law Enforcement, and Security from the office of the Under Secretary of Defense for Intelligence and Security, and Mr. Gurpreet Bhatia, Principal Director, Cybersecurity, office of the Chief Information Officer, served as the event's keynote speakers. During the ceremony, long-time DC3 veterans gave their recollections of key moments in our organization's history. Mr. Sunderbruch spoke to the future of DC3 and outlined the strategic plan for DC3's operations in 2023–2025.

CYBER FORENSICS LABORATORY

Cyber Forensics Laboratory (CFL)
CFL operates a state-of-the-art facility, using leading-edge technology and a technically diverse 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.

EXAM HIGHLIGHTS

Expert forensic technicians successfully repaired a chip from a car's infotainment system, recovering full GPS history and leading investigators to crucial evidence in a victim recovery case.

Examiners received a submerged cell phone with severe water-damage and corroded internal components. Technicians performed forensic repair and restored phone to operational state, resulting in successful analysis.

Completed
405
digital forensic exams

308
Exams completed involving systems and malware intrusions

883TBs
of data

2,524
evidence items

44%
of these exams involved crimes against children

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 Cyber Training Academy (CTA) and fraudulent activities.

1,600
hours of training to foreign partners

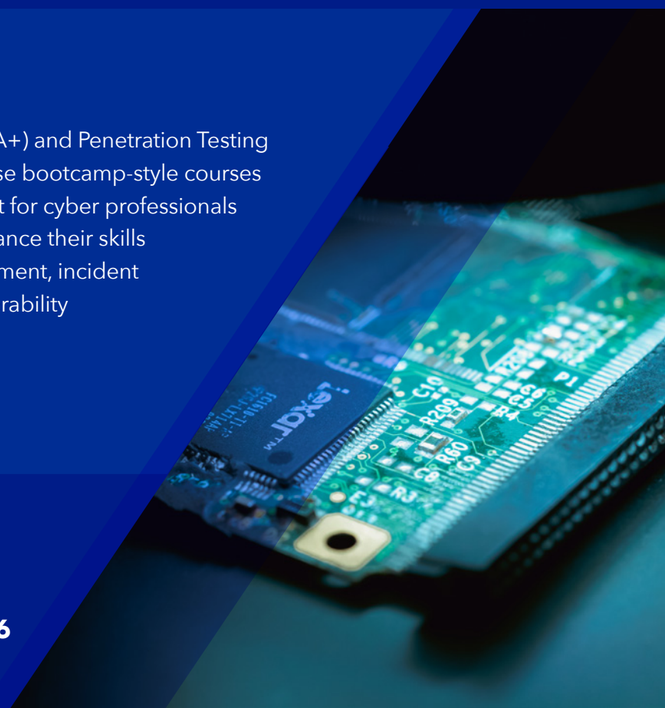
314,924
Training hours delivered

800
hours of on-demand training

10,083
Total CyberCasts

4,000
hours of mobile training teams deployment

Expansion of Cyber Training Offerings
CTA introduced Cybersecurity Analyst (CySA+) and Penetration Testing (PenTest+) into the catalog of offerings. These bootcamp-style courses contain the most up-to-date training content for cyber professionals looking to earn a certificate and further enhance their skills in security operations, vulnerability management, incident response, best practices for reporting, vulnerability scanning, communication code analysis, and uses for the various tools.



DIB CYBERSECURITY

DoD-Defense Collaborative Information Sharing Environment (DCISE)

As the operational hub for the DoD's Defense Industrial Base (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.

9%
increase in DIB Partnership to 1099 participants

Hosted
20
DIB Partner web conferences

Conducted
10
Analyst-to-Analyst (A2A) meetings with individual DIB Partners

Conducted
3
in-person Regional Partner Exchange (RPEX) events

Significant DCISE Operational Highlight

In October 2023, DCISE issued an alert to the DIB in response to a critical security incident involving Atlassian Confluence (CVE-2023-22515). The vulnerability threatened recent versions of the Atlassian Confluence Data, allowing unauthorized access to an attacker. DCISE swiftly disseminated vital information, including public and non-public indicators, to DIB Partners and the broader U.S. Government. Analysts utilized DCISE[3] to alert a targeted DIB company of nation-state activity, enabling them to halt data exfiltration as it was happening. The company shared detailed threat actor insights which enriched situational awareness for the DIB and DoD.

1,657
cyber threat reporting products

Total of
274,272
cyber threats were blocked from participants' firewalls

Approximately
90
threat indicator products sent to DIB Partners

Major DIB threat trend analysis in 2023:

- Potential foreign nation Advanced Persistent Threat (APT) activities
- DIB Partner infrastructure vulnerability to critical common vulnerabilities and exposures (CVEs)
- Data exfiltration incidents and data leaks
- Fake DoD Secure Access File Exchange (DoD-SAFE) website

INFORMATION TECHNOLOGY

In 2023, DC3 established the Directorate of Information Technology, which is composed of the Information Technology, Records Management, and Knowledge Management Divisions. The creation of the XT Directorate 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 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

Updates to DC3 Advanced Carver (AC)

AC is a highly capable digital content carving tool built for speed, accuracy, and extensibility (patent no. US10853177B2). DC3 has redesigned AC's technical capabilities introducing several new carving modules as well as improvements to the automated testing and security scanning (Sonarqube) processes built within.

Forensic digital video file carving continues to play a critical role in recovering data from corrupted, deleted, and fragmented digital storage devices. This carving tool aids forensic experts and investigators in their ability to reconstruct sequences of events and chronologies, uncover evidence that a user may have attempted to conceal, or help identify previously unknown victims.

Updates to the Electronic Malware Submission (EMS) System

EMS allows DoD Cybersecurity teams and partners a safe and secure portal to submit malware, network traffic, and volatile data to DC3's Cyber Forensics Lab (CFL) for examination. Submitters have the option of requesting an Automated Malware Response (AMR) available within minutes of submission or an in-depth examination by CFL's malware subject matter experts.

EMS improvements include: increased AMR submission size, file limits, and classification options; added Structured Threat Information eXpression (STIX) export options; clarified the types of examinations available to submitters; and expanded malware processing capabilities. These updates enable investigators and incident responders greater capability to more rapidly submit, define, and share standardized threat intelligence information in an industry-wide readable and consistent format.

OPERATIONS ENABLEMENT

Operational Enablement Directorate (OED)
OED integrates and contextualizes capabilities and data sources across DC3 to illuminate unique cyber risks and opportunities for U.S. Government 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.

PROJECT HIGHLIGHT

OED is developing a platform for the curation, sharing, and analysis of cyber-derived data—to include DC3- enabled sensoring—among partners. This development involves ensuring proper access controls, data tagging, and security controls to make operationally impactful data accessible and useable in a secure way. The platform was built in a cloud environment to allow for scalability and meets FEDRAMP Impact Level 5 (IL5) enhanced security standards suitable for National Security Systems (NSS) and systems containing LE sensitive data.

Produced
597
serialized intelligence products fusing DC3 and U.S. Government information

392
analytic engagements with U.S. Government Partners

235
Finished Intelligence citations across the interagency

Significant Operational Enablement Highlights
In an effort to rapidly innovate and deliver actionable insights, OED developed a cryptocurrency analytic capability to illuminate ransomware and cybercriminal activity leveraging digital assets. In 2023, OED cryptocurrency analysts identified $35 million in digital assets supporting ransomware operations.

In late-2022, OED was tasked to swiftly develop a program to place commercially provided sensors on DIB companies' networks. Operational development was done to reach an early 2023 fully functioning capability, resulting in achieving initial plan and acquisition process to operational award within the year.

VULNERABILTY DISCLOSURE

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

Significant Vulnerability Remediation
From October 2022 to July 2023, the VDP team encountered a security challenge when a white-hat researcher uncovered an Unauthorized Arbitrary File Upload and Deletion vulnerability. This vulnerability allowed the execution of an unauthenticated PUT method on the server. If exploited, this method posed a serious risk by permitting potential adversaries the ability to upload and delete HTML or JavaScript files on a US Government agency storefront. This specific security issue highlighted an incorrect access control vulnerability. These findings underscore the ongoing importance of rigorous cybersecurity practices along with vigilant monitoring to protect sensitive systems and data from evolving threats.

HACKER-POWERED SECURITY

49,318 Vulnerabilities (since launch)

5,527 Researchers (since launch)

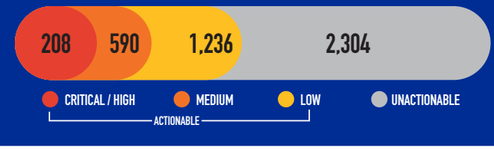
27,820 Successful Mitigated Reports (since launch)

New vulnerabilities (2023)	4,352
Actionable reports (2023)	1,975
Total attempted mitigations (2023)	2,723
Successful mitigated reports (2023)	2,380

2023 TOP COMMON WEAKNESS ENUMERATION'S (CWE)

CWE-200	Information disclosure	16,013
CWE-657	Violation of Secure Design Principles	6,041
CWE-79	Cross-Site Scripting (XSS)	5,975
CWE-284	Improper Access Control - Generic	2,048
CWE-601	Open Redirect	1,380

REPORT SEVERITY RATINGS



VDP Researcher of the Year 2023

Matt Moreschi, also recognized online as @pizzap0w3r or Pizzapower, commenced reporting to the DoD VDP in January 2021, contributing multiple findings of medium to critical severity. He exhibited exemplary responsiveness while collaborating with the DOD VDP team, submitting vulnerability reports characterized by their precision, clarity, high quality, and significant impact. Over a two-year period, he submitted 9 medium findings, 2 high, and 4 critical severity reports to the program. In July 2022, he actively participated in the Hack the U.S. bug bounty, presenting a high severity finding for Stored Cross-Site Scripting. Subsequently, in August and July 2023, he submitted 2 Remote Code Executions, 1 Authentication Bypass, and an account takeover, each having the potential for substantial impacts on systems and users. His approach showcased outstanding technical proficiency, featuring self-authored scripts and comprehensive documentation of each exploit in a lucid and accessible manner. In July 2023, he submitted 2 critical findings for authentication bypass and Remote Code Execution, by 3 medium findings, earning him the coveted July VDP Researcher of the Month accolade.

INTERNATIONAL ENGAGEMENT

1,600
hours of training to foreign partners

Hosted dignitaries from **7** foreign countries

EXTERNAL/ MEDIA AFFAIRS

DC3 leadership participated in numerous media endeavors with both national and local level media affiliates. Events included the Google Defense Forum, Women in Tech Symposium, and the Cybersecurity Executive Roundtable Forum.

Participated in approx 15 major media events

PARTNERSHIP ENGAGEMENT

In 2023, DC3 established the Directorate of Strategy and Partner Engagement (XE) by integrating the offices of Public Affairs, Plans and Policy, Organizational Development, and Executive Support Staff. The creation of XE unified elements dedicated within DC3 to providing organizational outreach and strategic engagement across the federal government and internationally.

In an effort to increase cross-collaboration and partnership initiatives throughout DC3, XE leaders established reoccurring core functional Mission Enablement Workshops to facilitate continued development of agency cohesion. Session curriculum aims to facilitate full-spectrum awareness of the organization by all employees.

98
internal/external engagements

500,000 X in
communication social media engagements

ENTERPRISE MANAGEMENT

Enterprise Management and Resources (ER)

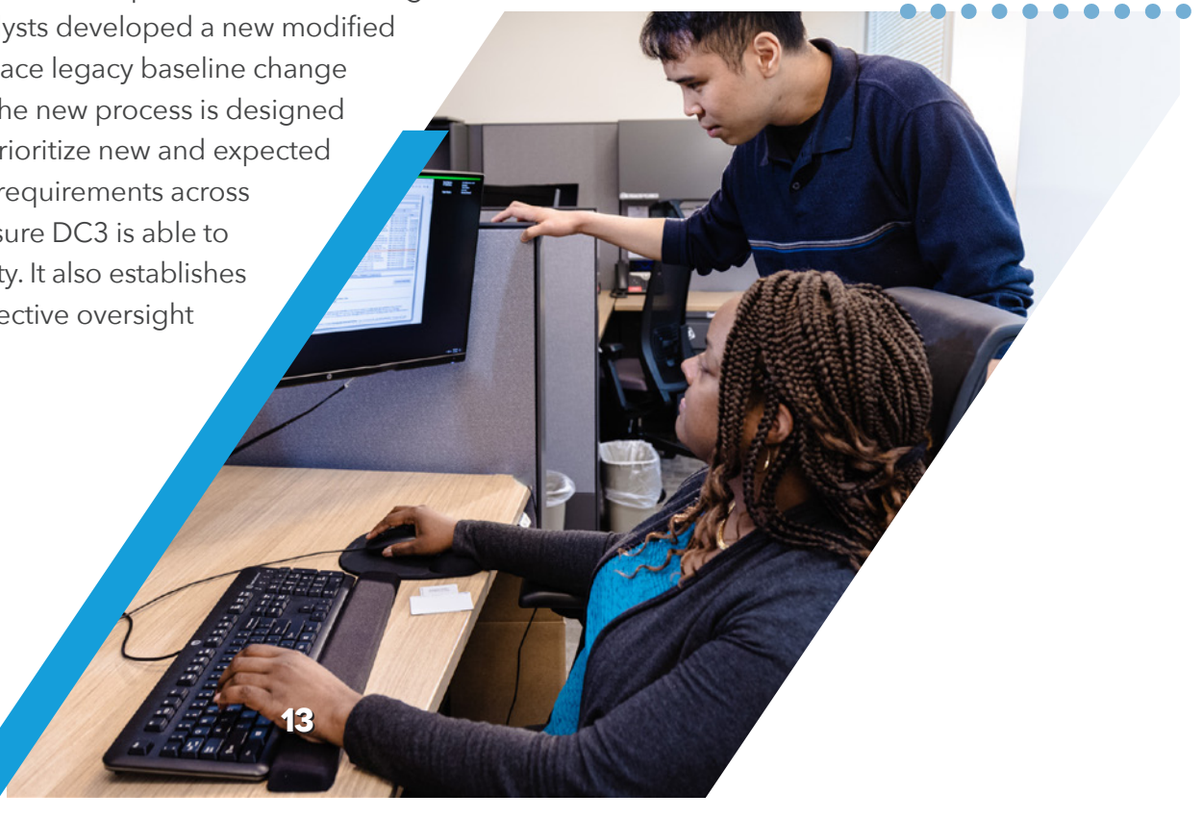
ER provides effective, efficient management of DoD/Air Force resources that are linked to strategic planning, budgeting, and performance reporting and serves as the command's focal point for contract, logistics, financial, program and requirements management and associated processes and controls.

Major Financial Projects

Structured alongside the new organizational realignment and mission expansions, and with effort to enhance cross-functional cooperation and nimble innovation, the ER Directorate began transitioning DC3 to a requirements-based organization with systematized project management.

The ER team facilitated critical enhancements to enterprise resourcing management tools that provide a standardized top-level summation of DC3 programs, projects, and initiatives. Enhancements will allow Executive leadership a more robust oversight of the DC3 portfolio and performance.

Focusing on alignment to critical requirements and funding efficiencies, program analysts developed a new modified process which would replace legacy baseline change requirement processes. The new process is designed to collect, manage, and prioritize new and expected mission internal/external requirements across the DC3 Enterprise to ensure DC3 is able to invest resources with agility. It also establishes program baselines for effective oversight of program health.



DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil
DC3.Information@us.af.mil

@DC3Forensics
DC3 Cyber Crime Center

Pub. Date 18 APR 2024