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.
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.

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.

Exam Highlights

- 405 digital forensic exams completed
- 308 exams completed involving systems and malware intrusions
- 883TBs of data
- 2,524 evidence items
- 44% of these exams involved crimes against children
Conducted in-person Regional Partner Exchange (RPEX) events
Conducted Analyst-to-Analyst (A2A) meetings with individual 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

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.

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 DCISE3 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.

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.
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.

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 2 critical findings for authentication bypass and Remote Code Execution, by 3 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 Execution, 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.
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

1,600 hours of training to foreign partners

Hosted dignitaries from 7 foreign countries

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 recurring 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.

500,000 communication social media engagements

PARTNERSHIP ENGAGEMENT

98 internal/external engagements
In an effort to enhance recognition, DC3 DEIA initiated a “Talks Series” which highlighted cultural and Barrier Analysis observances. Special guests included a virtual hosting focused on “Exploring Neurodiversity” from Dr. Margaret Swank, Associate Director of Psychological Health & Resilience Services, Office of Special Investigations. In a series of special recognition events, DC3 highlighted National American Indian Heritage Month (NAIHM) by welcoming SrA Danielle Dan and SSgt Garrett Anderlik to discuss their experiences in the Air Force and working with The Indigenous Nations Equality Team (INET).

DC3 council members collaborated and attended annual Air Force Office of Special Investigation’s DEIA Roundtable, an event that allowed DC3 and OSI to collaborate on key issues impacting DEIA efforts across the Department. The council maintained training compliance by attending various Diversity, Leadership, Diversity, and Barrier Analysis training such as the “Value Diversity and Culture” seminar.

Similarly, members reinvigorated attendance at the Air Force DEIA Conference, bi-monthly headquarters-level meetings, and monthly Air Force working groups, such as the Women’s Initiative Team (WIT).

In an effort to enhance future efforts, DC3 completed the Air Force Maturity Model to better understand and analyze implementing best practices and what barriers staff need to mitigate to enhance the diversity and equity footprint at DC3.