DoD CYBER CRIME CENTER



Mr. Eric Oliver
DC3 Chief Information Officer

DC3 Cyber Crime Center @DC3Forensics
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

UNCLASSIFIED

DoD CYBER CRIME CENTER (DC3)

1 of 6 Federal Cyber Centers critical to collaboration and coordination

SecAF is Executive Agent for DC3, DoW Digital/Multi-media (D/MM) Forensics

DoW Center of Excellence for D/MM forensics, cyber training, technical solutions (R&D), cyber analytics, and vulnerability sharing

Capabilities supporting DoW include:

- Cyber incident analysis/response and cyber threat intelligence sharing
- Enabling LE/CI investigations/operations, and Offensive/Defensive Cyber Operations
- Cybersecurity and Critical Infrastructure Protection
- Document and Media Exploitation (DOMEX) and Counterterrorism
- Technology Protection and Supply Chain Risk Management (SCRM)
- Illuminating advanced persistent/criminal threats via serialized/finished reports
- Innovative tool development, data standards, and capability integration

Lethality, Accountability, Readiness

UNCLASSIFIED



DC3 LINES OF EFFORT

Cyber Forensics Lab (CFL)

- Nationally accredited digital forensics lab
- Supports array of partners and classification levels
- Operating locations in San Antonio, TX and Atsugi, Japan

Cyber Training Academy (CTA)

- In residence, online, and mobile training teams
- Intermediate and advanced cyber courses
- LE/CI, Cyber Mission Force, and International Partners

Information Technology (CIO-CISO-XT)

- Modernize Global IT with a Cloud-First, Hybrid capabilities strategy
- Establish data governance--standardization, tagging, and info sharing
- Simultaneously operate, secure, defend, and extend networks/systems
- RDT&E of solutions for digital forensic and intrusion analysis



Industrial Base Collaboration (DCISE)

- Cybersecurity info sharing partnership with 1,300+ DIB companies
- Shares DIB and USG sourced cyber threat data
- Analysis and coordination for mandatory DIB cyber incident reports

Operations Enablement (OED)

- Sharply focused technical/cyber intelligence analysis
- Enable USG/DoW actions against cyber threats
- DoW solutions integrator in support of LE/CI/Cyber

Vulnerability Disclosure Program (VDP)

- Crowdsourced vulnerability reporting on DoW systems
- 5,800+ white-hat researchers from 45 countries
- Enduring partnership with USCYBERCOM/DCDC

Enterprise Management and Resources (ER)

- Managerial oversight of DC3 programs and projects
- Oversees budget, support contracts, performance, and logistics

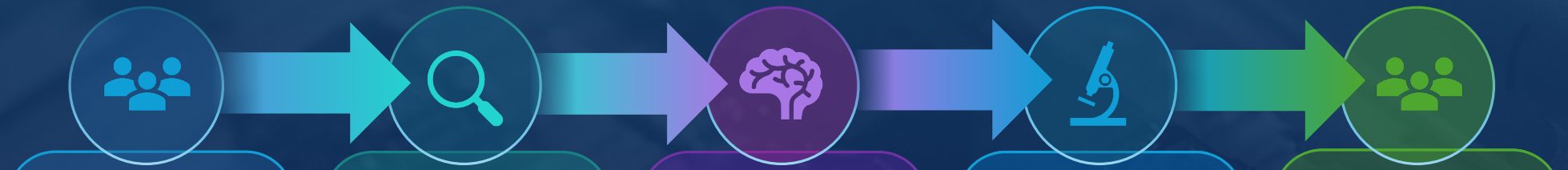
Strategy and Partner Engagement (XE)

- Deliberate efforts to enhance organizational cross-collaboration
- Integration of policy, strategy, public affairs, and engagements

UNCLASSIFIED

DCISE, OED, CFL: WORKING TOGETHER

FROM COLLECTION TO ACTIONABLE INTELLIGENCE



CYBER THREAT DATA SOURCES

- **DIB REPORTS** Voluntary/Mandatory Submissions
- **IC SHARING** Information Sharing with IC
- **OSINT/RESEARCH** Open Source Intelligence
- **REQUESTS** Support Team LE/CI Organizations

DCISE COLLECT & ANALYZE

- Ingest & Validate DIB Data
- Assess & Analyze Threat Information
- Produce Cybersecurity Reports
- Share with OED for Enhancement

OED ENHANCE & FUSE

- Analyst Research
- Foreign Language Enablement
- Intelligence Fusion & Correlation
- Enhanced Intelligence Products

CFL TECHNICAL VALIDATION

- Malware Analysis
- Hardware Analysis
- Forensic Exploitation
- Technical Validation & Attribution Support

SHARED INTELLIGENCE & MISSION PARTNERS

- **DIB CS PROGRAM REPORTING**
- **INTELLIGENCE PRODUCTS** Published to IC
- **INVESTIGATIVE LEADS** to Military, Civilian, & Allied Counterintelligence

UNCLASSIFIED

UNCLASSIFIED

CYBER TRAINING ACADEMY

From Collection to Actionable Intelligence

Design, develop, and deliver specialized cyber training to DoW, Federal LE/CI, and International partners.

- Resident, online, instructor-led virtual **delivery**
- **35 courses** with scalable course development
- Aligned and mapped to **8140 DCWF**
- **CompTIA** certification bootcamps

TRAINING FROM FOUNDATIONAL TO ADVANCED

CERTIFICATE – Cyber Activities Examiner

CERTIFICATE – Digital Media Collector

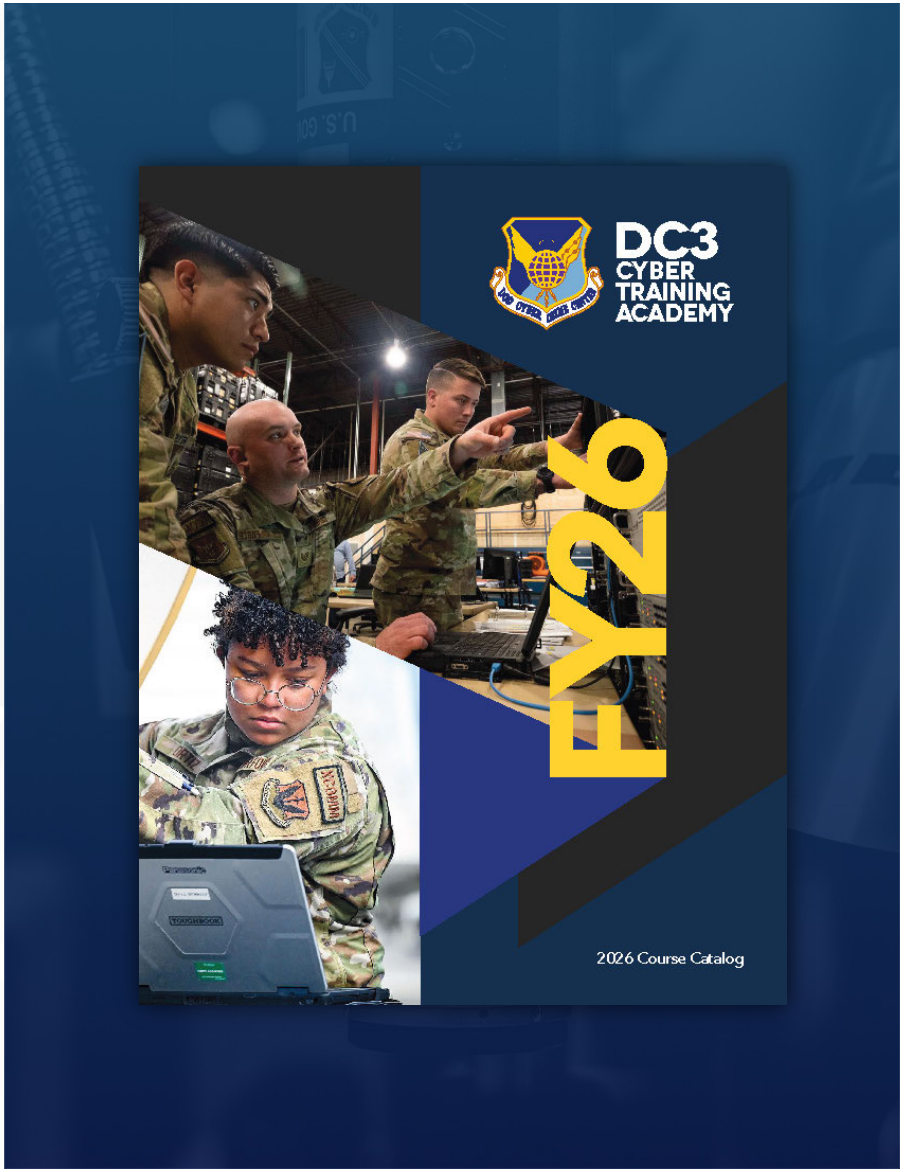
CERTIFICATE – Malware Analysis & Reverse Engineering

CERTIFICATE – Digital Forensic Examiner

CERTIFICATE – Cyber Fundamentals Certificate

CERTIFICATE – Cyber Crime Investigator

UNCLASSIFIED



UNCLASSIFIED

DC3 DATA INTEROPERABILITY VISION

DC3 HYBRID ENVIRONMENT

DATA SOURCES

OED Data
Intelligence Fusion & Correlation

DCISE Data
Voluntary/Mandatory Submissions

VDP Data
Vulnerability Reporting

CFL Data
Digital Forensics

DC3 DATA LAKE

DATA MESH

API ACCESS

DATA PRODUCT

PARTNER'S ENVIRONMENT

CYBERCOM:
Caspian Pigeon (HQ)
USCYBERCOM (DCDC)
ELICSAR (AFCYBER)

DCIOS/MDCOS:
NCIS
OSI
ACIC
ACID

OTHER PARTNERS:
NSA
DISA
ODNI
FBI

UNIFIED DATA
Integrating diverse data sources for a single operational picture.

SMARTER INTELLIGENCE
Enhancing, validating, and correlating data to generate actionable insights.

STRONGER PARTNERSHIPS
Securely delivering intelligence and data products to mission partners.

MISSION IMPACT
Driving faster decisions and operational advantage across the cyber enterprise.

UNCLASSIFIED



UNCLASSIFIED

INNOVATIVE STRATEGIC CYBER EFFORTS

Enable Insight and Action In Cyberspace and Beyond

Cryptocurrency Tracing Capabilities and Threat Intelligence

- Criminal organizations, ransomware groups, and nation-station actors targeting DIB, and critical infrastructure
- Cyber threat intelligence sharing with law enforcement partners
- Nation-state actors using criminal surrogates or criminal technics to conduct operations and criminal activities

Newly Deployed Agreement with U.S. Coast Guard (USCG)

- Operationalized Partnership: Analyst embedded to integrate maritime intelligence with military infrastructure defense
- Technology Threat ID: Advanced shared intelligence on nation-state actors targeting military OT architectures

Strategic Projects Aligned to Support U.S. Allied Partners

- Strategic operational efforts designed to elevate and enhance collaboration with global cyber partners
- Ongoing specialized efforts with France, Ukraine, and Oman
- Partnership with NCIS to establish Operating Location DC3 Pacific at (Naval Air Facility) Atsugi, Japan

ENSITE Sensor Program

- Singular commercial technology network sensor architecture for MDCOs
- Focused on Critical Programs and Technology DIB companies and MDCO interests
- Thwarted a ransomware attack in near real-time

UNCLASSIFIED



QUESTIONS AND OPEN DISCUSSION

Empowering Insight, Innovation, and Action for a Secure Cyberspace