DEPARTMENT OF DEFENSE CYBER CRIME CENTER

DC3 – Enabling Cyber Action

Terry Kalka
Director, DC3 DCISE

Agenda

- DC3 Overview and Lines of Effort
- Enabling Cyber Action
  - Defense Industrial Base – Vulnerability Disclosure Program (DIB-VDP)
  - Cyber Threat Information Sharing (DCISE)
  - Malicious Activity Detection and Response (ENSITE and DCISE^3)
  - Combatting Ransomware

EMPOWERING INSIGHT, INNOVATION, AND ACTION FOR A SECURE CYBERSPACE

DC3 Mission

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

What We Do

DC3 offers a range of integrated services, including cyber training, digital and multimedia forensics, vulnerability disclosure, cybersecurity support to the Defense Industrial Base, analysis and operational enablement, and advanced technical solutions and capabilities.

DoD Cyber Crime Center (DC3)

- One of seven Federal Cyber Centers designated by National Security Presidential Directive (NSPD) 54 – others are DNI CTIIC and IC-SCC, DOJ NCIJTF, DHS CISA, DoD USCYBERCOM and NSA
- DoD Center of Excellence for digital and multimedia (D/MM) forensics, cyber training, technical solutions, research and development, cyber analytics, and vulnerability sharing, in support of:
  - Law Enforcement and Counterintelligence (LE/CI)
  - Cybersecurity (CS) and Critical Infrastructure Protection (CIP)
  - Document and Media Exploitation (DOMEX) and Counterterrorism (CT)
- Integration of DC3 functions (lab, vulnerability disclosure, DIB Cybersecurity, analytics) often yields insight that:
  - Illuminates advanced persistent/criminal threats via serialized/finished report
  - Informs rapid updates to DC3 Cyber Training Academy offerings
  - Facilitates innovative tool development
- SECAF is DoD Executive Agent for DC3 and DoD D/MM Forensics

DC3 Lines of Effort

Cyber Forensics Lab (CFL)

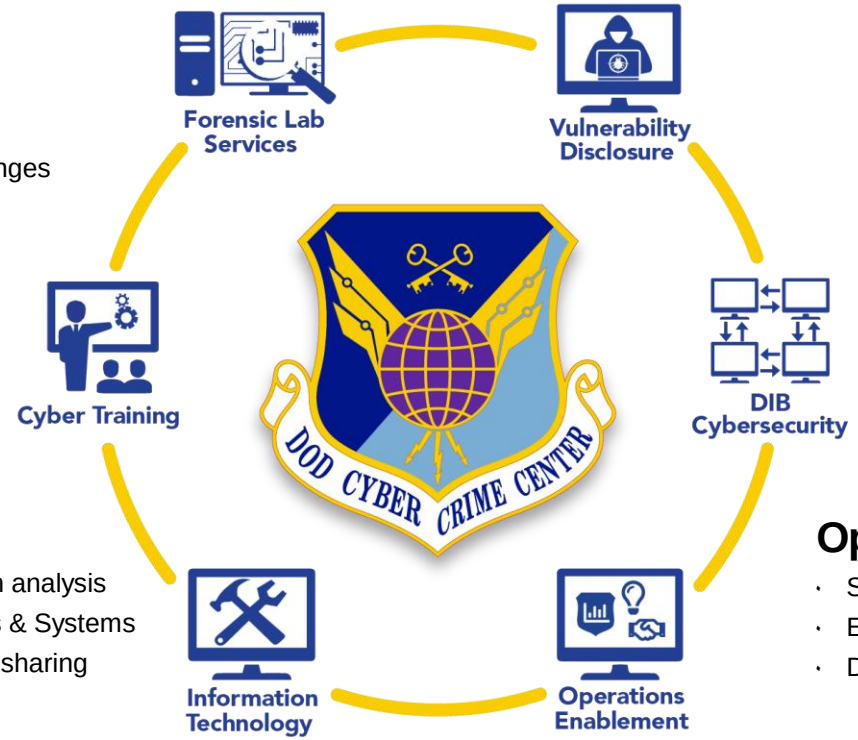
- Nationally accredited lab with sophisticated digital forensics
- Supports array of partners and classification levels
- Investment in tools and equipment to tackle toughest challenges

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 (XT)

- RDT&E of solutions for digital forensics exams and intrusion analysis
- Plan, Build, Operate, Secure, Defend, and Extend Networks & Systems
- Mission experts in data standards, tagging, and information sharing



Vulnerability Disclosure Program (VDP)

- Crowdsourced reporting of vulnerabilities on DoD systems
- 6,400+ white-hat researchers from 45 countries
- Enduring partnership with USCYBERCOM/JFHQ-DoDIN

Industrial Base Collaboration (DCISE)

- Cybersecurity partnership with 1,300+ defense contractors
- Voluntary and mandatory DIB incident repository
- Expanded cybersecurity offerings and partnerships

Operations Enablement (OED)

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

Enterprise Management and Resources (ER)

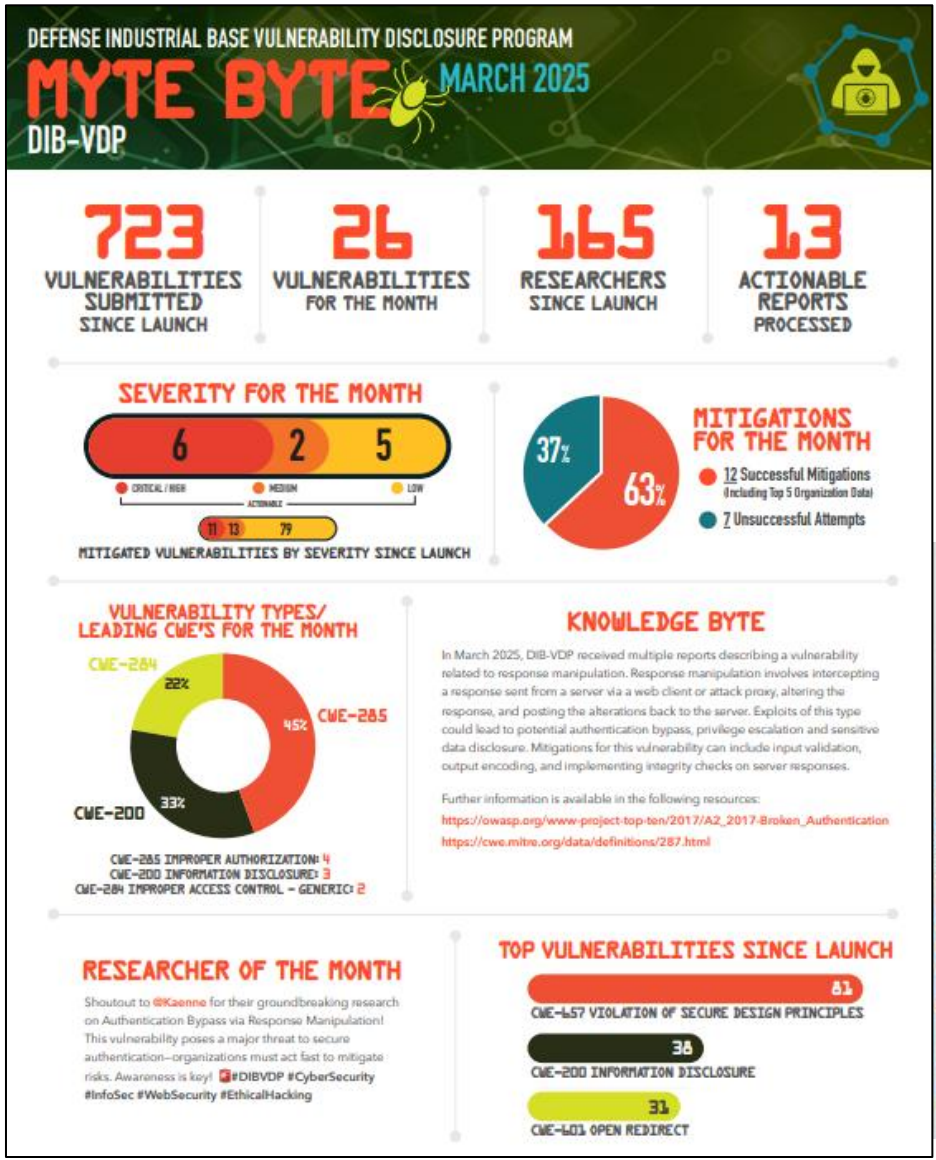
- Efficient and effective oversight of DC3 programs and projects
- Management of budgetary resources linked to requirements management, support contracts, performance reporting, logistics operations, and SAF engagement

Strategy and Partner Engagement (XE)

- Deliberate partnerships to enable action – share insights – efficiently reduce risk
- Policy, Planning, Strategic Communications and Engagements, and Organizational Development

Defense Industrial Base – Vulnerability Disclosure Program

- Collaboration with DCSA
- Pilot in 2021-2022
- Enduring capability launched in 2024
- 723 vulnerabilities reported
- 103 vulnerabilities mitigated
- Cost of average data breach in 2024 = $4.88M*
- **~$503M saved in incident response**



*-https://www.ibm.com/reports/data-breach

Cyber Threat Information Sharing

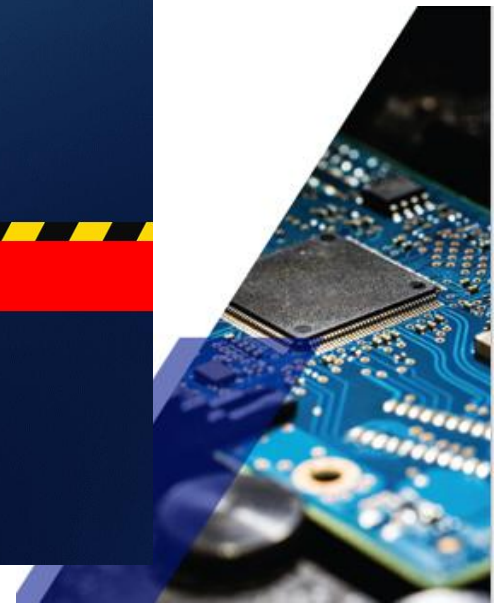
- **D**oD-DIB **C**ollaborative **I**nformation **S**haring **E**nvironment (DCISE)
- Reporting, information sharing, and engagements with 1,300+ DIB companies
- DCISE^3 (“dice cubed”) blocks 46,000 threats per month
- FY 24 Stats:
  - 1,600 cyber threat products
  - 44,000 indictors of compromise
  - 46 Alerts
  - 133 TIPPERs
- All-time stats (through 2024):
  - 15,000 cyber threat reports
  - 746,000 IOCs
  - 79,000+ hours of non-cost forensic and malware analysis for DIB Partners

Malicious Activity Detection and Response

- **E**nhanced **N**etwork **S**ensor & **I**ntelligent **T**hreat **E**numeration (ENSITE)
  - On-net sensoring
  - Real-time threat intelligence
  - AI/ML-powered detection
  - Alert Scoring Triage
  - Centralized Dashboard

- **DCISE³** (“dice cubed”)
  - Analyzing logs from 350+ DIB firewalls
  - Automated threat scoring from open source and USG information
  - Auto-block of high-scoring threats
  - Enables pro-active threat hunting

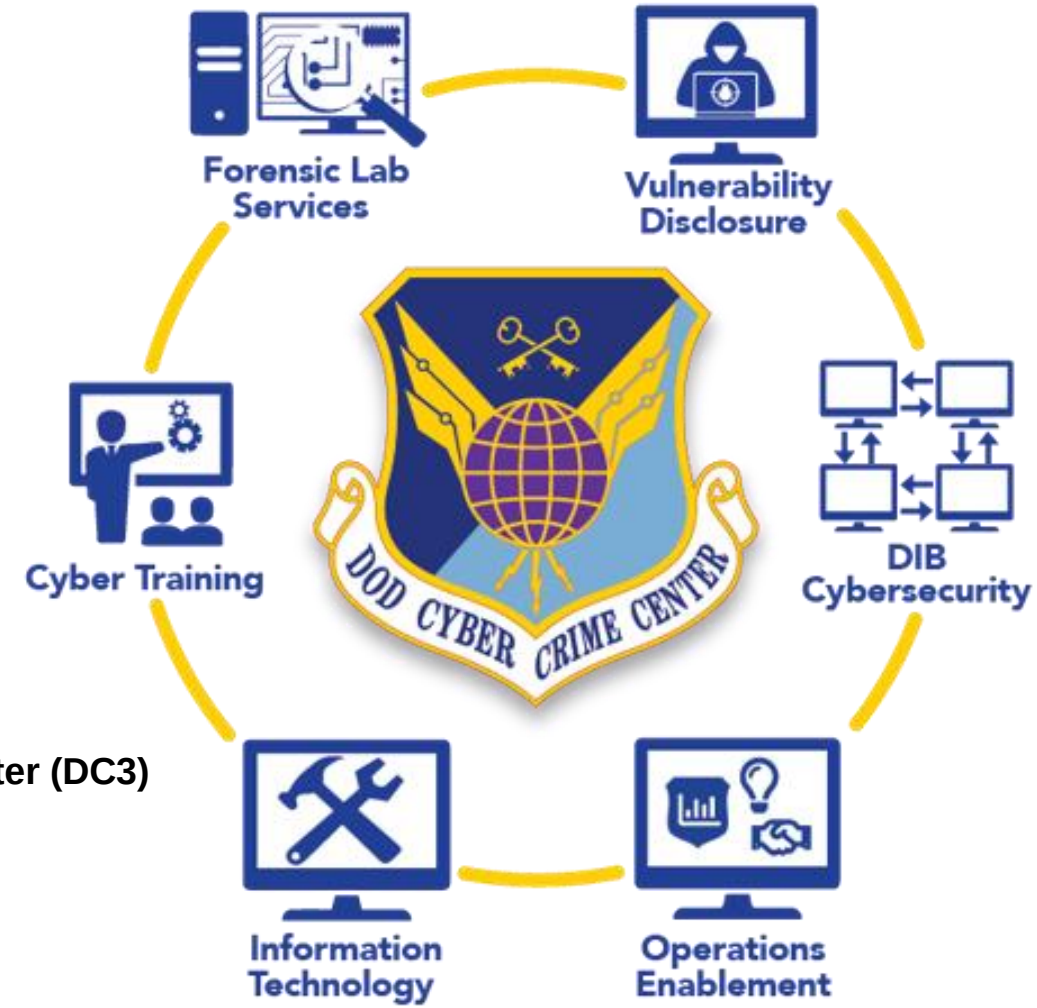
Combatting Ransomware



Key Takeaways

- DC3 is Federal Cyber Center and DoD Center of Excellence in digital and multimedia (D/MM) forensics, cyber training, technical solutions, research and development, cyber analytics, and vulnerability sharing
- DIB-VDP detects and mitigates publicly exposed vulnerabilities
- ENSITE and DCISE^3 enable real-time detection and blocking of malicious activity
- DC3 enables cyber action in collaboration with a broad range of cybersecurity and law enforcement partners

Thank You



Department of Defense Cyber Crime Center (DC3)
410-981-6610
Email: dc3.information@us.af.mil
X/Twitter: @DC3Forensics
LinkedIn: @defense-cyber-crime-center

Terry Kalka
Director, DC3 DCISE
terrance.kalka@us.af.mil