# DoD CYBER CRIME CENTER: Securing the Defense Ecosystem

**Mr. Terry Kalka**
*Director, DC3 DCISE*

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

# Agenda

- Introduction
- DC3 Overview and Lines of Effort
- Defense Industrial Base (DIB) Cybersecurity)

# Terry “TK” Kalka

- **Director, DC3/DCISE**
- **IT Professional since the late 20th century**
- **Cybersecurity Professional since October 9, 2012**
  - Integration of Cyber, Intelligence, and Operations
  - Protection of critical assets
  - The Defense Ecosystem

# 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*

# 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

## Enterprise Management and Resources (ER)

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


## 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

## Strategy and Partner Engagement (XE)

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

# Partnerships and Collaborations



# Perspectives on the DIB

## Supercharge the U.S. Defense Industrial Base

*2026 National Defense Strategy, Line of Effort 4*

## The Defense Industrial Base

**"The set of domestic and foreign companies or organizations—at all levels—that performs research and development, design, production, delivery, and maintenance of DoD systems, subsystems, and components or parts, as well as those that provide software and other critical services to meet U.S. defense requirements."**

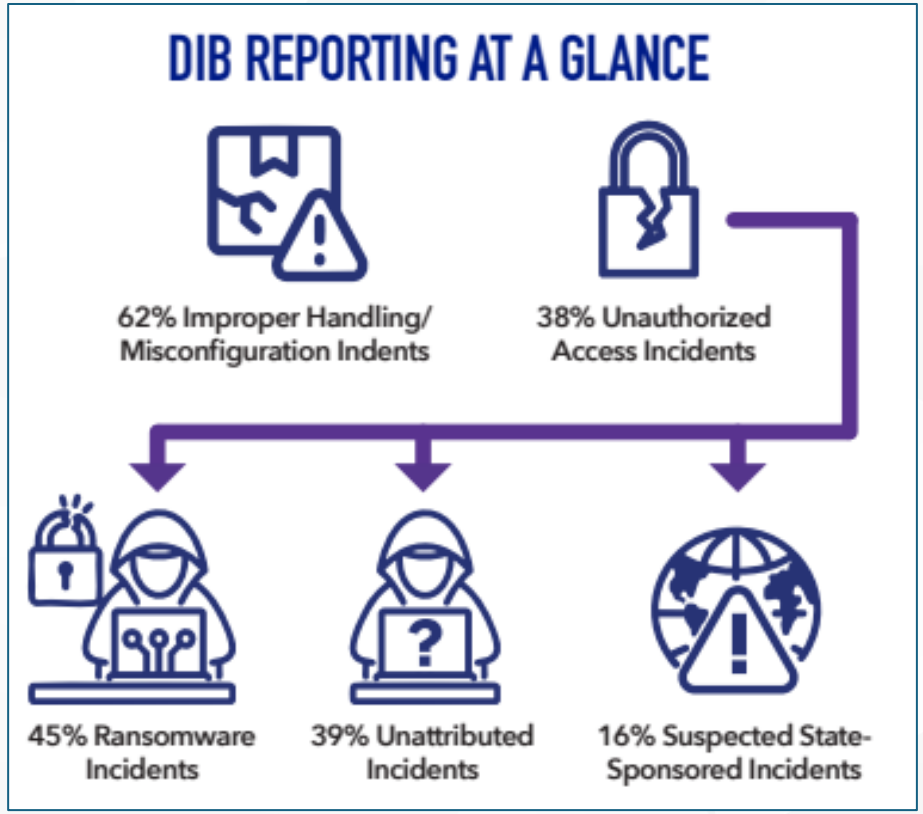
***2024 DoD DIB Cybersecurity Strategy***

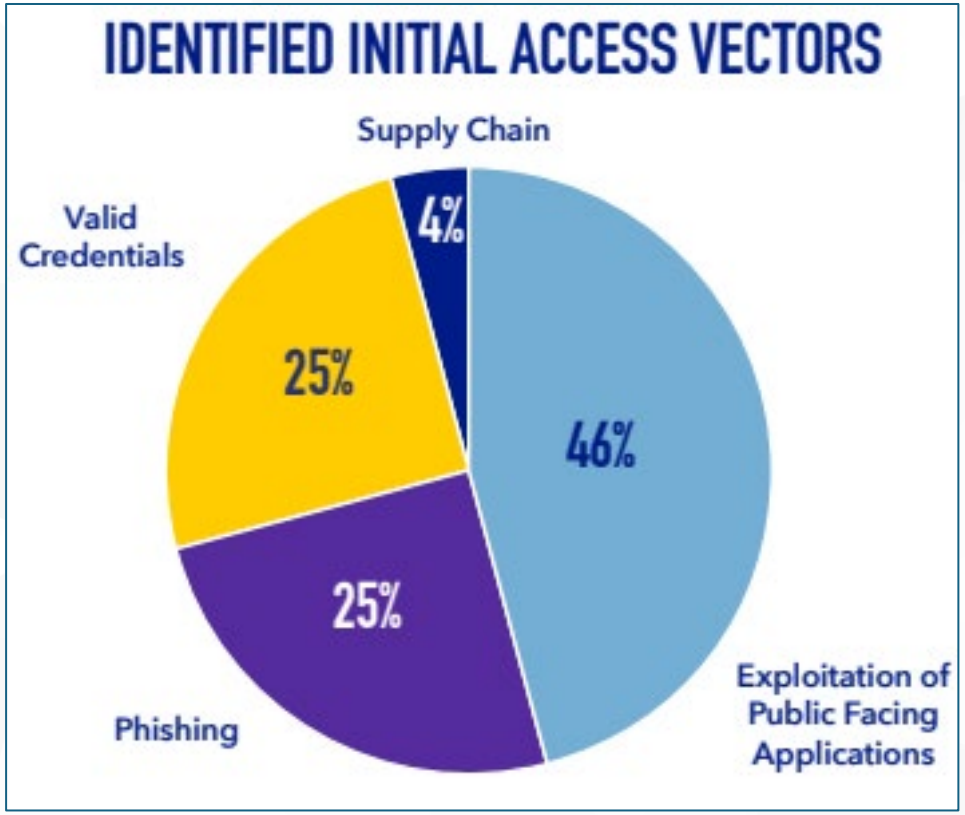
## The Defense Ecosystem

**"…the Department of Defense, the defense industrial base, and the array of private sector and academic enterprises that create and sharpen the Joint Force's technological edge."**

***2022 National Defense Strategy***

# Perspectives on the Threat




Increased Reporting ◆ Increased Severity
Ransomware ◆ Data Loss
Disrupted Operations ◆ Acquisition Dollars



Q1, Calendar Year 2026
more available at https://www.dc3.mil

# Defense Industrial Base Collaboration

- **DoD-DIB Collaborative Information Sharing Environment (DCISE)**
  - Executes **DIB Cybersecurity Program** established by 32 CFR Part 236
  - Voluntary participation governed by Framework Agreement
  - Information sharing, threat awareness, and engagements with 1,300+ DIB companies (Partners)
  - Unless waived, information sharing is anonymous
- **Information shared (including/combining USG and DIB sourced information)**
  - FY 25: 1,260 cyber threat products, 131,000 indictors of compromise, 132 TIPPERs
  - All-times: 17,525 cyber threat reports, 820 IOCs, 110,000+ hours of no-cost forensic and malware analysis for DIB Partners

# Cyber Threat Analysis

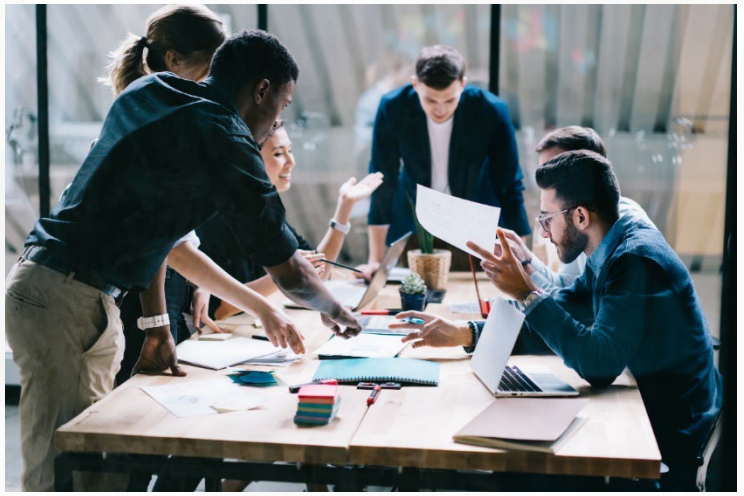
- **How does DCISE collect information?**
  - Incident Collection Format (ICF)
    - Voluntary (DoD's DIB CS Program)
    - Mandatory (DFARS 252.204-7012)
  - Cybersecurity capabilities (see next slides)
  - USG reporting
  - Open source research

95% of our threat data is **not** commercially available

- **How does DCISE share information?**
  - Encrypted email (in an emergency we'll call you)
  - Cybersecurity capabilities (see next slides again)
  - Collaboration events – come to us, or we'll come to you
  - In development: automated info sharing via MISP/TAXII

# Focused Collaboration

- **DC3 facilitates meaningful collaboration events for DIB and USG Partners:**
  - Technical Exchange (TECHEX)
  - Analyst-to-Analyst (A2A) Meetings
  - Regional Partner Exchanges (RPEX)
  - Web Conferences and SVTCs
  - Facilitated Incident Response Exercises (DCISE FIRE)
  - Requests for Information (RFIs) – send them to dc3.dcise@us.af.mil

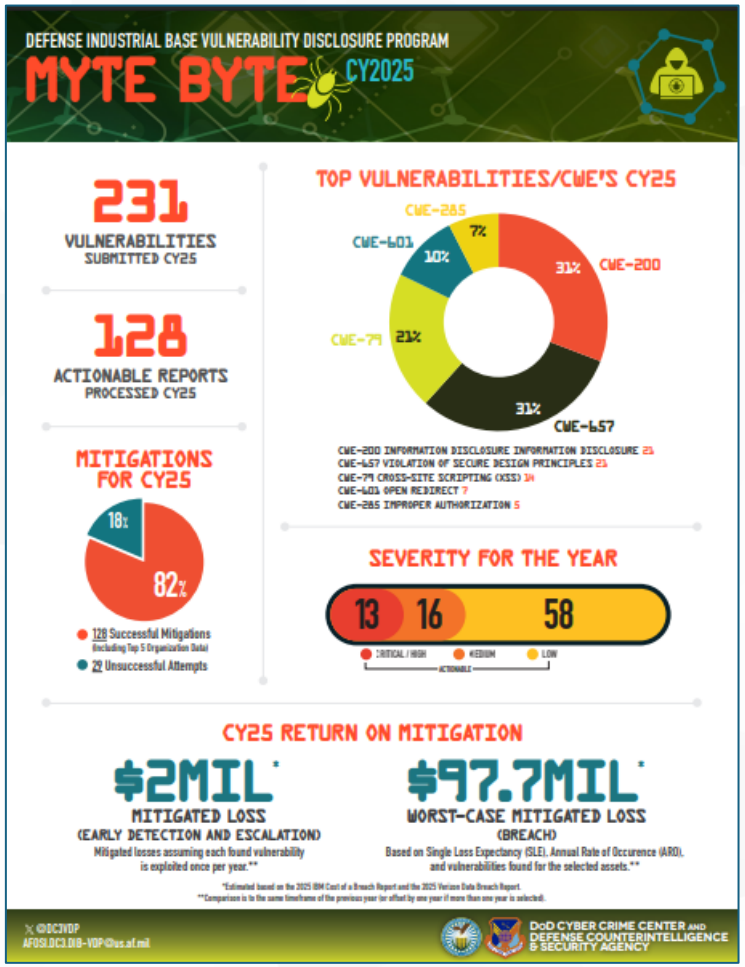


# Malicious Activity Detection, Analysis and Response

- **Electronic Malware Submission/Automated Malware Response (EMS/AMR)**
  - Online submission of malware to DC3: https://ems.dc3on.gov
  - Receive automated response providing information about malware
- **DCISE³ (“dice cubed”)**
  - Analyzing logs from 350+ DIB firewalls
  - Automated threat scoring from open source and USG information
  - Auto-block of high-scoring threats
    - Blocks 46,000 threats per month
- **Enhanced Network Sensor & Intelligent Threat Enumeration (ENSITE)**
  - On-net sensoring of encrypted data packet flow
  - Real-time threat intelligence
  - AI/ML-powered anomaly detection
    - Alert Scoring Triage
    - Centralized Dashboard

# Defense Industrial Base – Vulnerability Disclosure Program

- **Collaboration with DCSA**
- **Pilot in 2021-2022**
- **Enduring capability launched in 2024**
- **CY 25 Metrics:**
  - 231 vulnerabilities submitted
  - 128 vulnerabilities mitigated
- **Cost of average data breach in 2025 = $10.22M***
- **~$1.3B saved in incident response**




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

# Voluntary Participation

- **DIB CS Program Participants are Defense Contractors working with CUI**
  - And their subsidiaries
  - And their MSP/MSSP/TPSP
  - And their supply chain partners
- **Large, mid, and small-sized defense contractors**
- **Sole source providers, market competitors, joint-development partners, supply chain partners**
- **Manufacturers of weapon systems, platforms, and critical parts**
- **Commercial solution and service providers**
- **Federally Funded Research and Development Centers (FFRDCs)**
- **University Affiliated Research Centers (UARCs)**

# Join the DIB CS Program!

## Improve Your Cybersecurity Posture and Operational Resilience by Joining the DIB Cybersecurity Program!

- Handle DoD CUI in support of a DoD contract
- Have or acquire DoD-approved medium assurance certificates to enable encrypted unclassified information sharing (https://cyber.mil/eca/)
- Execute the Framework Agreement (FA) with DC3 by contacting…

# DC3.DIB.CSRegistration@us.af.mil

# Mandatory Cyber Incident Reporting

- **Applies to all contracts with DFARS 252.204-7012 (most DoD contracts)**
- **Cyber incidents affect:**
  - Covered contractor information system, or
  - Covered defense information, or
  - Contractor's ability to perform operationally critical functions
- **Initial report must be submitted within 72 hours of discovery**
- **Follow-on reports strongly encouraged**
- **Affected media must be preserved for 90 days to allow for DoD to request submission**
- **Cloud Service Providers to DoD report per DFARS 252.239-7010**
- **Reported through Incident Collection Format (ICF) portal –**

**https://dibnet.dod.mil**

# Key Takeaways

- DC3 is a 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

- DC3 enables cyber action in collaboration with a broad range of cybersecurity and law enforcement partners

- DC3 DCISE is the focal point for DIB Mandatory Incident Reporting and sustains a voluntary cybersecurity partnership with over 1,300 DIB entities


# QUESTIONS

*Empowering Insight, Innovation, and Action for a Secure Cyberspace*

**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**