DoD Cyber Crime Center

A Federal Cyber Center

DCISE 101

DoD Cyber Crime Center (DC3)

A Federal Cyber Center

Cyber Forensics Lab (CFL)

- Nationally accredited lab with exquisite digital forensics
- Support range of military operations and classifications
- Federated forensics and DC3 Pacific

Cyber Training Academy (CTA)

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

Information Technology (XT)

- R&D of software and systems solutions
- Electronic Malware Submission, DC3 Advanced Carver
- Federated approach to standards, tagging, information sharing

Vulnerability Disclosure Program (VDP)

- Crowdsourced vulnerabilities on DoD systems
- 5,000 white-hat researchers from 45 countries
- Strong partnership with USCYBERCOM/JFHQ-DoDIN

Industrial Base Collaboration (DCISE)

- Cybersecurity partnership with 1,000+ CDCs
- Voluntary/mandatory DIB incident repository
- Expanded cybersecurity offerings

Operations Enablement (OED)

- Sharply focused technical/cyber intelligence analysis
- Counter FIE threats to DoD, USG, and DIB
- DoD solutions integrator in support of LE/CI/Cyber

Strategy and Partner Engagements (XE):

Deliberate partnerships to enable action - share insights - efficiently reduce risk

Operational Element of DoD's DIB CS Program

Designated as the single DoD focal point for receiving all cyber incident reports affecting DIB unclassified info/networks

Voluntary reporting responsive to the DIB CS Framework Agreement

- A public-private partnership enabling:
  - Analytic support and forensic malware analysis for the DIB
  - Increased USG and industry understanding of cyber threat (analytic products, semi-annual technical exchanges, etc.)
  - Enhanced protection of unclassified defense information
  - *Confidentiality of shared information*

Mandatory reporting responsive to:

- DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*
- DFARS Clause 252.239-7010, *Cloud Computing Services*
- 32 CFR Part 236, *DIB Cyber Security Activities,* and others

DoD's DIB Cybersecurity (CS) Program

A public-private cybersecurity partnership established by DoD CIO and executed by DC3:

- Provides a collaborative environment for sharing unclassified and classified cyber threat information
- Offers analyst-to-analyst exchanges, mitigation, remediation strategies, Cybersecurity-as-a-Service
- Provides analytic support and forensic malware analysis to DIB Partners
- Protects confidentiality of shared information
- Increases US Government and industry understanding of cyber threats
- Enables companies to better protect unclassified defense information on company networks or information systems

Mission: Enhance and supplement Defense Industrial Base (DIB) participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems

Participation

- DIB CS Participants are CDCs*:
  - Large, mid, and small-sized defense contractors
  - Sole source providers, market competitors, joint-development partners, supply chain vendors
  - Manufacturers of weapon systems, platforms, and critical parts
  - Federally Funded Research and Development Centers (FFRDCs)
  - Commercial Solution and Service Providers
  - University Affiliated Research Centers

** - pending update to CFR 32 pt. 236, anticipated in CY 2024*

Info Sharing & Collaboration

DIB NETWORK

Online incident reporting and access to DCISE threat products (NIPR & SIPR instances)

DIB TECHNICAL WEB/ TELECONFERENCES

DIB Partners and DCISE Analysts address current adversary techniques and trends

A2A AND B2B MEETINGS

Tailored to Partner capabilities, threats, and dynamic cybersecurity considerations

TECHEX AND RPEX/VIPEX

Interactive forums for deep technical discussion on a wide variety of cyber threat related topics

CYBERSECURITY as a SERVICE (CSaaS)

No cost cybersecurity services to identify gaps in cyber resiliency and provide technological capabilities

PRODUCTS

Cyber threat products, warnings, and notices to strengthen cybersecurity

- **Analysis of nation-state Advanced Persistent Threat (APT) DIB cyber events since February 2008**
  - Performed ~ 79,000 hours of no-cost forensics and malware analysis
  - Published ~ 15,000 cyber reports
  - Shared ~ 610,000 actionable, non-attributional indicators
  - Informed by multiple USG data streams (USIC, LE, CI, and industry cyber threat reporting)

Cyber Threat Information Sharing

- **DIBNet-Unclassified (DIBNet-U)**: Unclassified PKI-protected web portal used by the DIB to report cyber activity, and includes new participant application process, document libraries, and cyber threat collaboration tools

- **Classified Cyber Threat Products:** Dissemination of classified Secret level cyber threat information incorporate multiple methods to include: Technical Exchanges (TechEx), Regional Partner Exchanges (RPEX), Analyst to Analyst (A2A) Engagements, Distribution via Classified Media, DC3/DCISE SIPR Intelink, Secure Phone & Fax.

DCISE CTI Products

- **DCISE Produces 12 different products ranging from indicator-based to strategic cyber threat analyses**
  - **Threat Information Product (TIP)**
    - Derived from USG reporting; includes relevant IOCs to DIB/CDCs and narrative context
  - **Customer Response Form (CRF) Rollup/Supplement**
    - CRF Rollup – Derived from DIB reporting; includes relevant IOCs to DIB/CDCs and narrative context
    - CRF Supplement – Produced when additional amplifying data becomes available after initially reported in CRF Rollup (i.e. malware samples)
  - **Cyber Targeting Analysis Report (CTAR)**
    - In-depth risk analysis product detailing adversarial cyber targeting of US DoD technology/platforms/systems
  - **Threat Activity Report (TAR)**
    - In-depth analysis of cyber threat actors' TTPs against DIB targets
  - **DCISE Notifications**
    - Alerts, Warnings, Advisories, TIPPERs, Cyber Incident Notifications (CINs)
    - Vehicles to notify DIB Partners of varying levels of cyber threats (critical through situational)
  - **Weekly Indicator Round-Up (WIR)**
    - Roundup of DCISE IOCs released in DCISE products for the given week
  - **Cyber Threat Round-Up**
    - Compilation of relevant cyber news articles, posted to DIBNET splash page
  - **Slick Sheets (on varying topics)**

DCISE Expanded Offerings: Cyber Resilience Analysis (CRA)

- Interview-based analysis of organization's current CS resilience posture
- Collection of 300 questions in 10 security domains
- Questions mapped to CMMC, NIST 800-171, NIST Cybersecurity Framework domains, and the Cybersecurity Framework Profile for Ransomware Risk Management
- Facilitated analysis over 6–8 hours in person or virtually
- Final report highlights strengths and weaknesses
- Partners who have repeated CRAs have seen a 90% increase in compliance for underperforming domains

DCISE Expanded Offerings
Cybersecurity as a Service

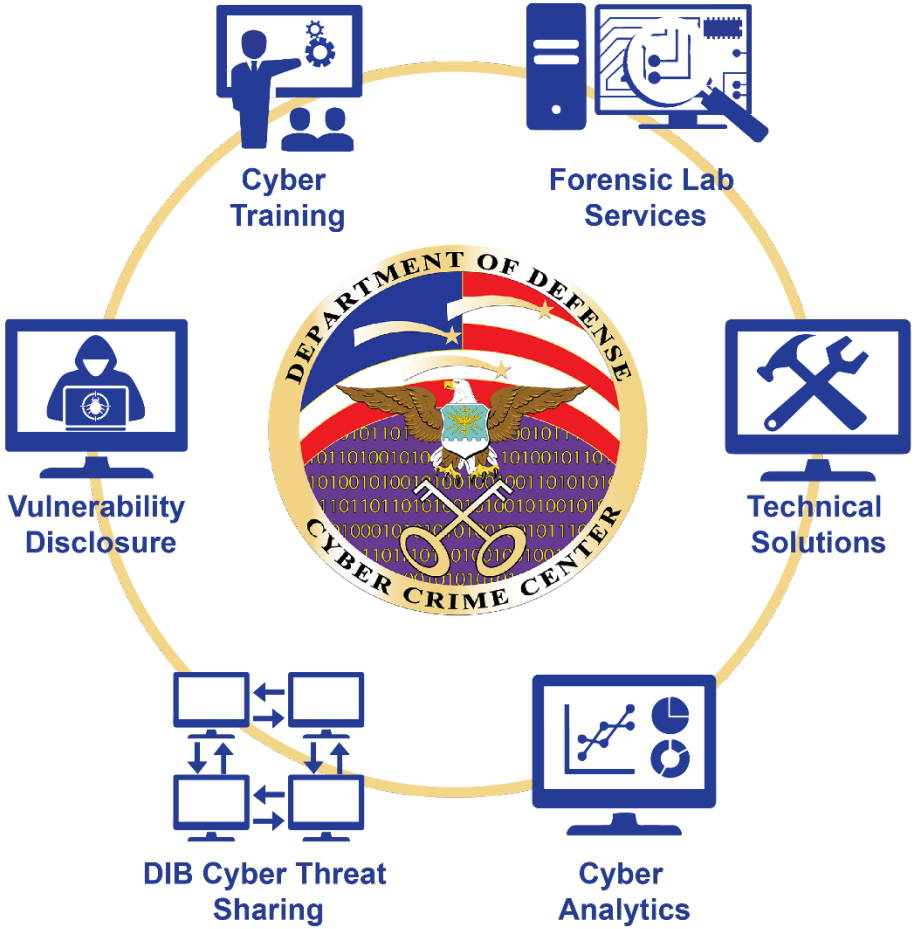
DCISE³

- Compares DIB Partner firewall logs to DIB, USG, and commercial threat feeds
- Individual dashboards for DIB Partners
- Anonymized aggregated dashboards for DCISE analysts
- Auto-blocking feature supported on compatible firewalls
- Identified previously unknown vulnerable corporate assets
- Enabled proactive tipping to DIB Partners for instances of IOT vulnerabilities, SolarWinds compromises, Fortigate vulnerabilities, Confluence 0-days, ProxyShell targeting, malicious scanning activity
- Proved 80% uniqueness in DCISE indicators

Adversary Emulation

- A form of penetration testing
- Leverages adversarial tactics, techniques, and procedures
- Test of DIB Partner security controls and policies against the most likely adversary to target them

Questions?



Scott Taylor
scott.taylor.55@us.af.mil
Desk: 410-981-6688

dc3.dcise@us.af.mil
DCISE Hotline: (410) 981-0104
Toll Free: (877) 838-2174
Web: www.dc3.mil
on Twitter @DC3DCISE