DoD Cyber Crime Center

A Federal Cyber Center

DC3 and the Defense Industrial Base: Cooperating to Secure the Defense Ecosystem

Mr. Terry Kalka

Director, DC3 DCISE

Agenda

- Background on the DoD Cyber Crime Center (DC3)
- Perspectives on the Defense Industrial Base (DIB)
- DoD's DIB Cybersecurity (CS) Program
- The role of DC3 DCISE
- Capabilities and offerings

DC3

A FEDERAL CYBER CENTER

Enable insight and action in cyberspace and beyond.

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.

DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)

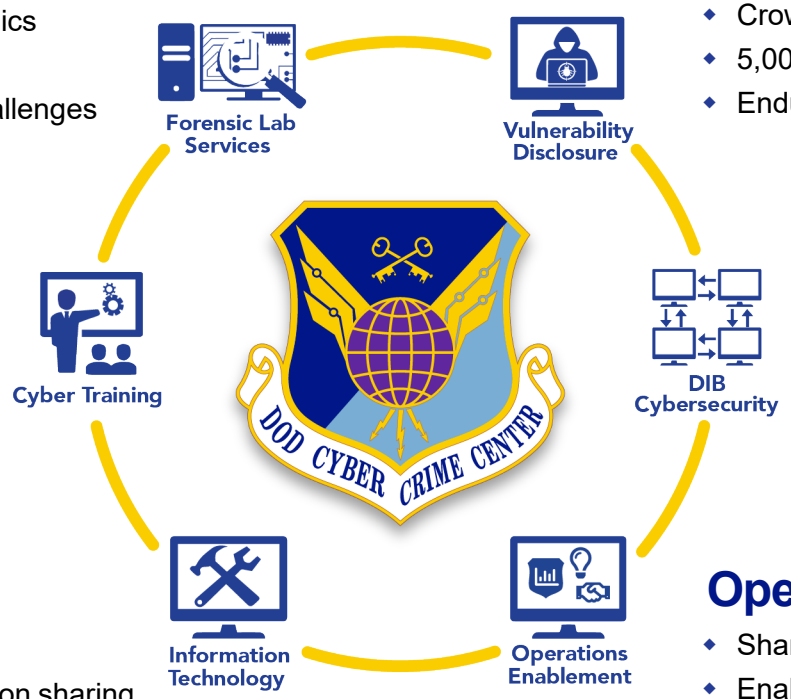
A Federal Cyber Center

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

Vulnerability Disclosure Program (VDP)

- Crowdsourced reporting of vulnerabilities on DoD systems
- 5,000+ white-hat researchers from 45 countries
- Enduring partnership with external and foreign partners



Cyber Training Academy (CTA)

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

Industrial Base Collaboration (DCISE)

- Cybersecurity partnership with 1,000+ companies
- Voluntary and mandatory DIB incident repository
- Expanded cybersecurity offerings and partnerships

Information Technology (XT)

- R&D and deployment of software and systems solutions
- Federated approach to standards, tagging, and information sharing

Operations Enablement (OED)

- Sharply focused technical/cyber intelligence analysis
- Enable actions to mitigate/address cyber threats
- DoD solutions integrator in support of LE/CI/cyber

Strategy and Partner Engagement (XE)

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

What is the Defense Industrial Base?

- **2024 DoD DIB Cybersecurity Strategy:**
  - **The set of domestic and foreign companies or organizations – at all levels – that perform research and development, design, production, delivery, and maintenance of DoD systems, subsystems, and components or parts, as well as those provide software and other critical services to meet U.S. defense requirements**

- **2022 National Defense 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**

Today's Environment

- DoD relies upon the DIB to develop and produce innovative and advanced technologies, so warfighters have every available battlefield advantage
- DoD provides DIB companies with sensitive, unclassified information as a necessary function
- Adversaries, nonstate actors, and cyber crime organizations seek to exploit the DIB and its sensitive information
- Public/private (Government/DIB) collaboration is essential to securing sensitive data within the DIB

DoD's DIB Cybersecurity (CS) Program

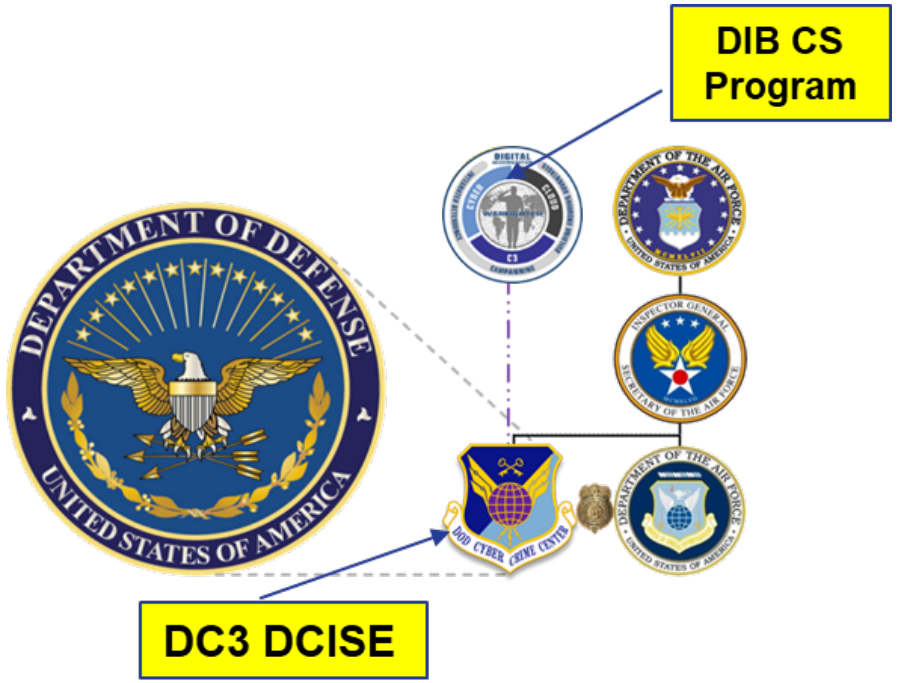
- **A public-private cybersecurity partnership established by DoD CIO and executed by DC3:**
  - **Provides a collaborative environment for sharing cyber threat information**
  - **Analyst-to-analyst exchanges, mitigation & remediation strategies**
  - **Protects confidentiality of shared information**
  - **Increases US Government and industry understanding of cyber threats**
  - **Open to Cleared Defense Contractors (through April 10, 2024)**
  - **All contractors who store or process Covered Defense Information (effective 11 Apr 2024)**

Voluntary Participation

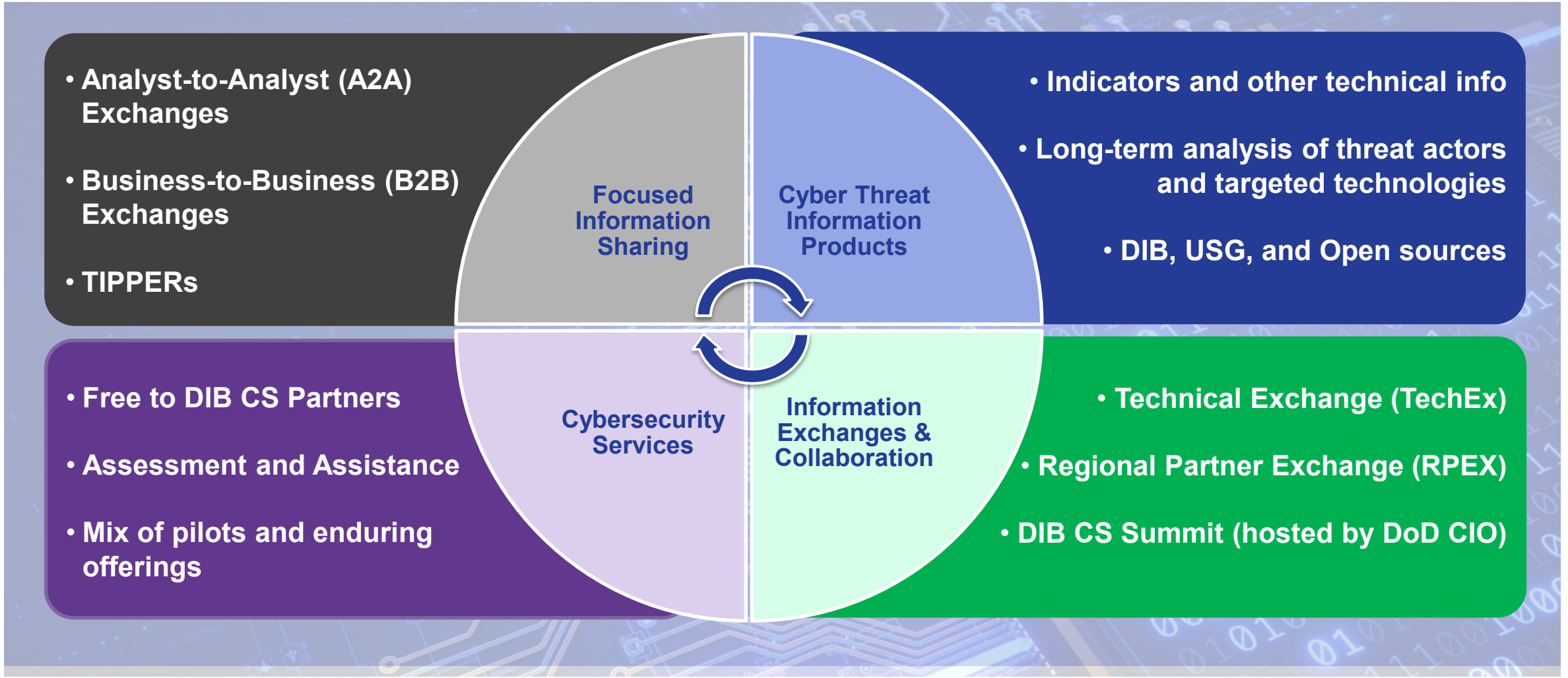
- **DIB CS Program Participants are Defense Contractors:**
  - Cleared Defense Contractors (through April 10, 2024)
  - All contractors who store or process Covered Defense Information (effective April 11, 2024)
  - Large, mid, and small-sized defense contractors
  - Sole source providers, market competitors, joint-development partners, supply chain vendors
  -
  - Manufacturers of weapon systems, platforms, and critical parts
  - Commercial solution and service providers
  - Federally Funded Research and Development Centers (FFRDCs)
  - University Affiliated Research Centers (UARCs)

What is DC3 DCISE?

- DoD-DIB Collaborative Information Sharing Environment
- A directorate within the DoD Cyber Crime Center (DC3)
- The operational arm of the DIB CS Program



DC3 DCISE Products, Services, and Activities



Cyber Threat Analysis

- **How does DCISE collect information?**
  - **Incident Collection Format (ICF)**
    - **Voluntary (DoD's DIB CS Program; referred to as VOL-ICF)**
    - **Mandatory (DFARS 252.204-7012; referred to as MIR-ICF)**
    - **Cybersecurity as a Service (CSaaS) Offerings (more in subsequent slides)**
    - **USG Reporting**
    - **Open source research**

- **DIB CS Program = Crowd Sourcing**
  - **"A rising tide lifts all boats"**
  - **Activity blocked at one firewall may be missed by others**
  - **Value of the Program can be enhanced by increased participation**

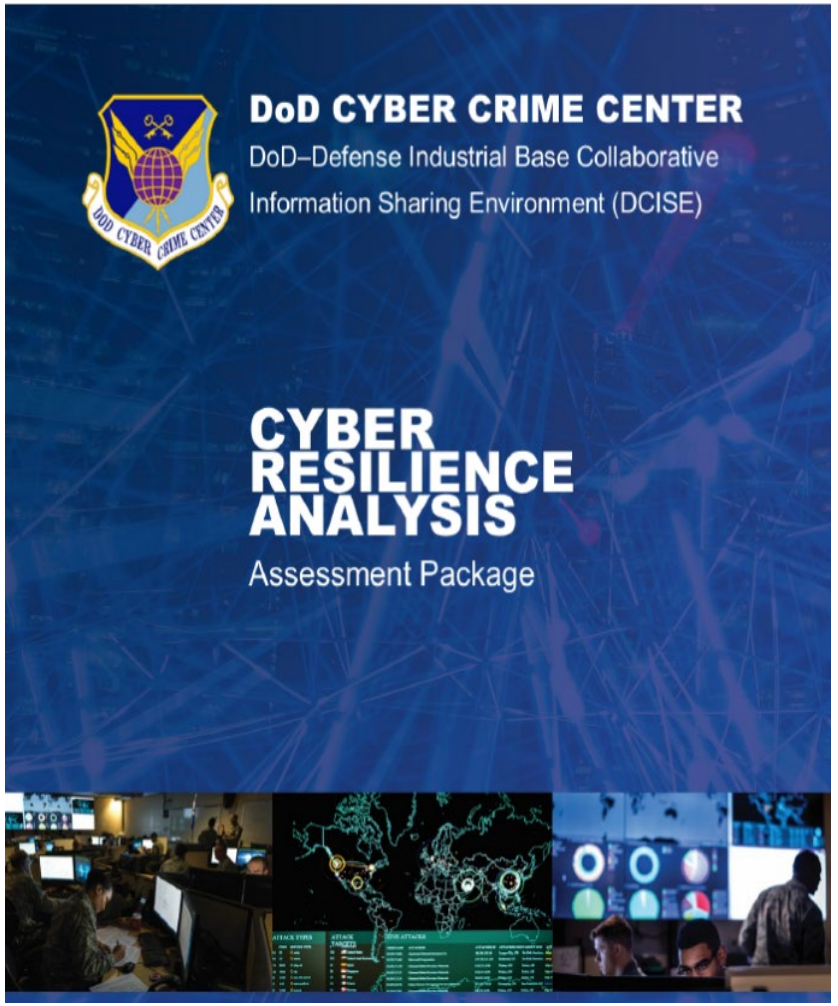
Focused Collaboration

- DCISE facilitates meaningful collaboration events amongst Partners and/or Government through a variety of options:
  - Technical Exchange (TECHEX)
  - Analyst-to-Analyst (A2A) Meeting
  - Business-to Business (B2B) Meeting
  - Regional Partner Exchanges (RPEX)
  - Virtual Industry-Based Partner Exchanges (VIPEX)
  - Webconferences
  - Support of Sub-Working Groups
  - Requests for Information (RFI)
  - DIBNet Forums
  - Polls and Surveys

- Partner Management personnel are always available to assist with coordination.

Cyber Resilience Analysis (CRA)

- **Establishes baselines** for process maturity, operational resilience, and cyber risk management by **analyzing processes and practices** related to a *specific critical service*
- **No cost, lightweight PDF tool - 299 questions spanning 10 security domains**
  - **In-person or virtual facilitation (up to 8 hours), or self assess**
  - **Final report with analyst debrief**
- **Analysis based on:**
  - **NIST SP-800-171 (172 and R3 in-progress) and the Cybersecurity Framework**
  - **NIST profile for ransomware risk management**
  - **CMMC v2.0 (in-progress)**



DCISE³

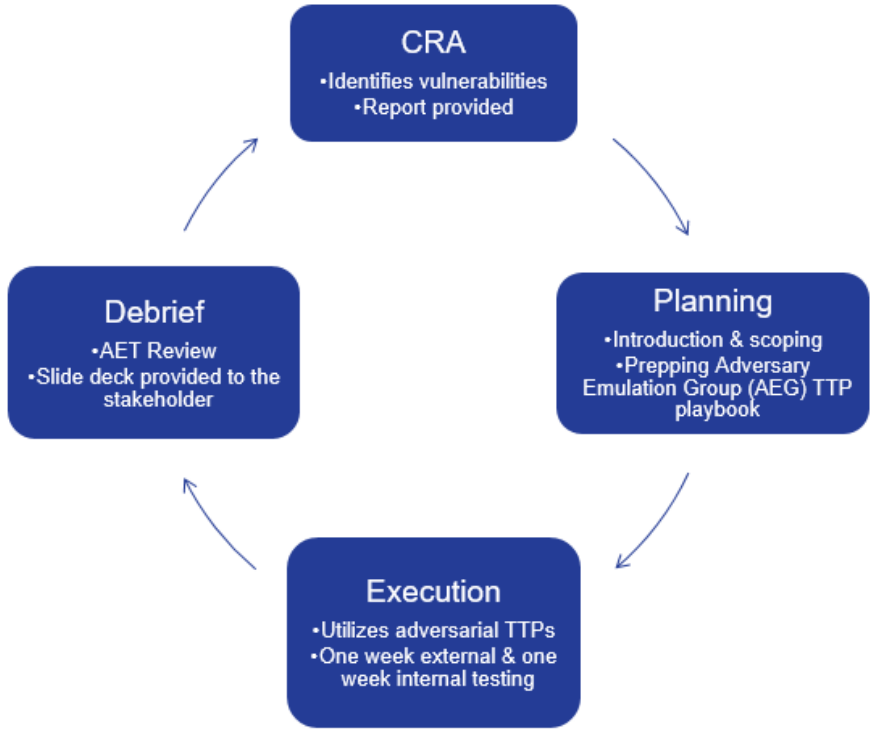
A non-invasive, fully automated complement to your existing cyber defense posture using DCISE cyber threat information and Celerium technology

- Zero cost to DIB CS Partners
- No hardware required = No impact to network performance
- Optional auto-blocking of threats
- Automated threat scoring & triage
- Automated delivery of DCISE indicators of compromise and commercial threat intelligence
- Helps protect DoD information within DIB networks
- Supports NIST SP 800-171
- Enables proactive threat hunting
- Informs DCISE notifications and threat products
- Strong cybersecurity protections

Adversary Emulation Test

- **A threat-informed penetration test that leverages DCISE analysis and uses adversarial tactics, techniques, and procedures (TTPs) in a controlled environment**

- **Produces both actionable and measurable reporting that assists DIB Partners proactively strengthen their overall cyber defense posture and the protection of sensitive DoD information**

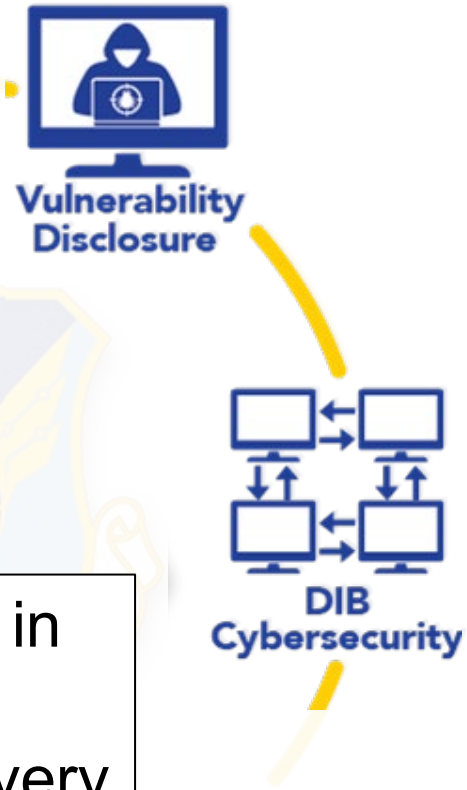


"You discovered blind spots that our previous $40,000 pen test did not reveal." - DIB Partner

"Our managed service provider felt pressure to do well on the test, and as a result the scheduled AET lit a fire under them to 'prepare for heavy weather' and ensure our system had all the corrections we had requested prior to the AET." - DIB Partner

DIB-Vulnerability Disclosure Program (VDP)

- **Built on the successful 2021-2022 pilot (and the DoD-VDP)**
- **White-hat researches + Public-facing infrastructure = Vulnerabilities!**
- **Reported, validated, and sent to DIBCo for remediation**
- **Remediation validated prior to close-out**
- **Details to be announced April 2024**



Pilot Outcomes:

1019 Vulnerability Reports Total
41 Small/Medium DIB Companies
368 DIBCO Assets researched by
288 crowd-sourced ethical hackers
403 Actionable Reports, **100%** closed out

$**1.8b saved** in DIB response/recovery costs

Joining the DIB CS Program

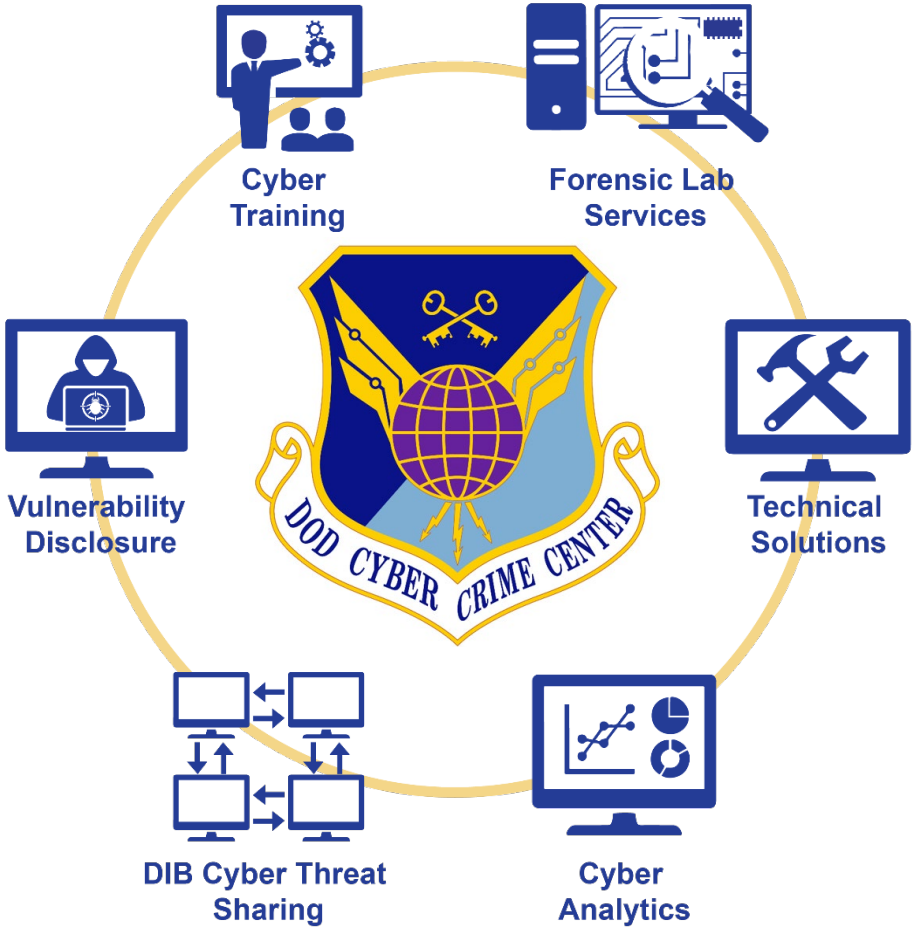
1. Acquire an External Certification Authority (ECA) certificate* from a vendor through https://public.cyber.mil/eca/
2. Apply at https://dibnet.dod.mil/dibnet/company-application
3. Sign the Framework Agreement (+ amendments as needed)
4. Attend onboarding sessions

* - Changing from Medium Assurance Certificates to Procurement Integrated Enterprise Environment (PIEE) - *although published in the Federal Register, this change will not be immediate*

Key Takeaways

- Cyber attacks are a real and present danger to the Defense Industrial Base and to National Security
- DIB Cybersecurity is a DoD priority
- 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
- DC3/DCISE operates the DIB CS Program in partnership with DoD CIO
- DC3 offerings are available to DoD contractors that transmit CUI…
  - And their subsidiaries
  - And their MSPs
  - And their supply chain partners
- The way ahead requires continual public/private engagement and collaboration

Questions?



Terry Kalka
Director, DC3 DCISE
terrance.kalka@us.af.mil
410-981-1163