A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

THE THREAT IS REAL

Malicious cyber actors work around the clock to intrude on your network, compromise and steal data, and bleed your organization of trade secrets and intellectual property. Cyber threats to Defense Industrial Base (DIB) unclassified information networks represent an unacceptable risk of compromise of Department of Defense (DoD) information and pose an imminent threat to US national and economic security interests.

DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Program

DoD's DIB CS Program is a unique public-private cybersecurity partnership and voluntary cyber threat information sharing program. It was established by the DoD to enhance and supplement participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems. Through collaborative cyber threat information sharing and Cybersecurity as a Service (CaaS) capabilities, the program improves DIB network defenses, reduces damage to critical programs, and increases cyber situational awareness.

The Program

- Offers actionable information, mitigation, and remediation strategies
- Increases US Government (USG) and industry understanding of cyber threats
- Enables Partners to better protect unclassified defense information
- Protects confidentiality of shared information

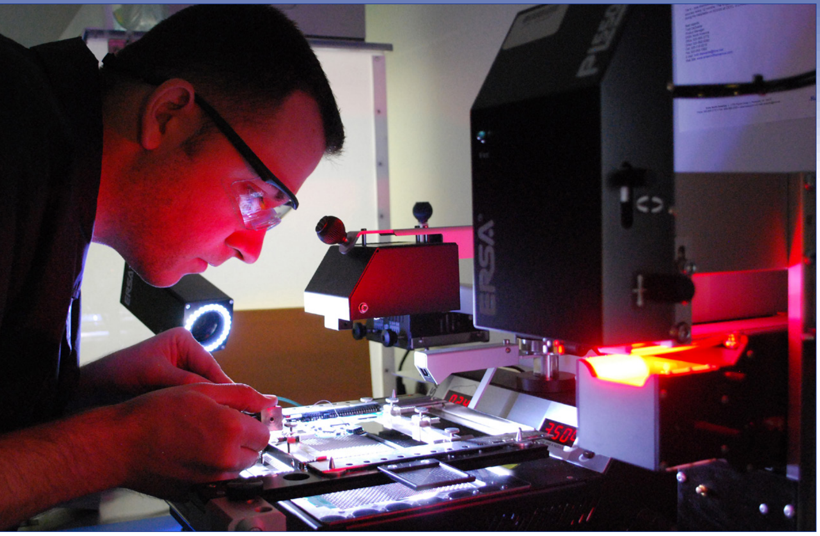
Value of Participation

- Collaborative partnership with more than 920 Cleared Defense Contractors (CDCs) and USG agencies
- Engagement opportunities at many levels between USG and DIB, from the C-suite to analyst level
- Access to indicator and threat products created from DIB reporting, multiple USG data streams, and
    - ~534,600+ actionable, non-attributable (to submitting source) indicators
    - ~78,700+ hours of no-cost forensics and malware analysis for Partners
    - ~12,750+ cyber threat reports

How do I join?

To be eligible to participate in the program, DoD contractors must be a CDC and:

- Have an existing Facility Clearance (FCL) granted under NISPOM (DoD 5220.22-M)
- Execute the standardized Framework Agreement (FA) with the USG
- Have, or acquire, DoD-approved medium assurance certificates to enable encrypted unclassified information sharing



> *"The ability of the United States to maintain readiness, and to surge in response to an emergency, directly relates to the capacity, capabilities, and resiliency of our manufacturing and defense industrial base and supply chains."*
>
> **–Executive Order 13806**

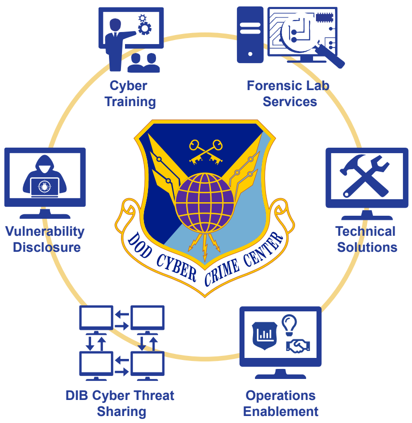
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

LET'S REDUCE RISK TOGETHER

DCISE and the DIBNet portal are the entry points for Cybersecurity as a Service (CaaS) and both mandatory (Defense Federal Acquisition Regulation Supplement [DFARS]) and voluntary cyber incident reporting under DoD's DIB CS Program. DCISE develops and shares actionable threat products, and performs cyber analysis, diagnostics, and remediation consults for DIB Partners. In addition, DCISE coordinates malware analysis and intrusion forensics with DC3's Cyber Forensics Laboratory.

Through knowledge and situational awareness from DCISE products and services, DIB CS Program Partners benefit from a stronger security posture and are able to better protect their networks and information systems from Advanced Persistent Threats (APTs) and others seeking to steal DoD information and intellectual property.

DC3 CAPABILITIES



Operations Enablement Directorate (OED): OED performs sharply focused technical analyses to support the cyber investigations and operations of Law Enforcement and Counterintelligence (LE/CI) agencies including AFOSI, NCIS, and FBI, and provides subject matter expertise on APT groups. Integrates disparate and emerging technologies to enhance collaboration, interoperability and the collective capabilities of DoD and Federal, LE/CI, cybersecurity and acquisition communities.

Cyber Forensics Laboratory (CFL): The lab performs D/MM forensics examinations, device repair, data extraction, and provides expert testimony for DoD. CFL performs the malware and system image analysis for the mandatory and voluntary DIB submissions.

Cyber Training Academy (CTA): The academy provides classroom and web-based cyber training to DoD elements that protect DoD information systems from unauthorized, criminal, fraudulent, and foreign intelligence activities. CTA confers DoD certifications in digital forensics and cyber investigations.

Technical Solutions Development (TSD): TSD tailors software and system solutions to support digital forensic examiners and cyber intrusion analysts, including OED, DCISE, and CFL, with tools and techniques engineered to their specific requirements. Some of these tools and techniques can be found on GitHub's public repository. TSD has also developed the Electronic Malware Submission Portal, where approved users with valid PKI certificates can submit exams to the system.

Vulnerability Disclosure Program (VDP): The Secretary of Defense directed DC3 to begin VDP operation in 2016. Supporting the DoD Chief Information Officer, US Cyber Command, Joint Force HQs – DoDIN, and the cyber elements of all DoD components, the VDP crowdsources the expertise of private-sector cyber security researchers to identify vulnerabilities on DoD information systems.

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS) MANDATORY REPORTING

DoD contractors are required to report cyber incidents under DFARS. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, defines adequate security, controlled technical information, cyber incidents, technical information, and reporting requirements. Any contractor safeguarding DoD unclassified controlled technical information must be familiar with the requirements of DFARS 252.204-7012 and where to access additional information.

Learn more about DFARS 252.204-7012:
https://www.acq.osd.mil/asda/dpc/index.html

Report mandatory cyber incidents to DCISE via the DIBNet portal: https://dibnet.dod.mil/portal/

Learn more about the DIB CS Program:
https://dibnet.dod.mil/

Pub Date: 23 March 2022