A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD–Defense Industrial Base Collaborative Information Sharing Environment

DCISE FACT SHEET

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE)–DCISE is the operational hub of the Defense Industrial Base (DIB) Cybersecurity Program of the Department of Defense, focused on protecting intellectual property and safeguarding DoD content residing on, or transiting through, contractor unclassified networks. The public-private cybersecurity partnership provides a collaborative environment for crowd-sourced threat sharing at both unclassified and classified levels. DCISE provides cyber resilience analyses for Cleared Defense Contractor (CDC) companies, and offers unmatched Cybersecurity-as-a-Service capabilities. DCISE performs cyber threat analysis and diagnostics, offers mitigation and remediation strategies, provides best practices, and conducts analyst-to-analyst exchanges with DIB participants ranging in size from small to enterprise-sized companies.

DC3/DCISE is the reporting and analysis hub for implementation of Title 10 U.S. Code Sections 391 and 393 regarding the reporting of certain types of cyber incidents by CDCs, and the related Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012). Cyber incidents outlined in the DFARS are submitted to DC3/DCISE as mandatory reports; however, all other cyber activity can be reported voluntarily.

- Rated at the “Defined” level (Maturity Level 3) for Capability Maturity Model Integration for Services (CMMI-SVC)
- Oversees a collaborative partnership with over 1,003 CDCs and U.S. Government (USG) agencies
- Has shared over 589,006 (and counting) actionable, non-submitting-source-attributable indicators
- Provides no-cost forensics and malware analysis for DIB Partners (over 78,822 hours thus far)
- Disseminates (over 13,863 to date) cyber threat reports for both DIB and USG consumption (DIB partners access DCISE reporting via their DIBNET accounts, and USG members can access via SIPRNet Intelshare)
- Operates a 24/7/365 support hotline (1-877-838-2174) to assist submitters and DIB and USG Partners

> *“The threat is real. By sharing our findings, we can reduce risk together.”*
>
> —DCISE

DCISE CAPABILITIES

Analytics Division (AD): The AD conducts analysis on cyber activity submitted by DIB Partners, the DoD, and other USG agencies to develop a complete understanding of known or potential threats to unclassified DoD information residing on or transiting DIB systems and networks. The AD also analyzes aggregate data from DIB Partner incident reports to produce technical analysis products and presentations, and provide other threat mitigation resources. The division collaborates with liaison officers from USG agencies to create and maintain technical and multi-source threat profiles. The Analytics Division is comprised of three branches:

1. **Daily Operations Branch:** processes both voluntary and mandatory incident reports on a daily basis, conducts malware analysis, compiles Customer Response Form (CRF) Rollups, produces Threat Information Products (TIPs), and engages with DIB Partners. In follow-up to its processing of incident reports, this branch maintains regular contact with personnel from the affected CDC in order to gather additional necessary information.

2. **Threat Notification Branch:** conducts mid-range analysis, producing the following threat products: Alerts, Warnings, Advisories, TIPPERs, and other threat-based analyses. To share valuable information with the DIB, this branch requests the downgrade and release of classified information derived from USG sources. Such information is shared in various cyber threat products.

3. **Strategic Analysis Branch:** conducts long-range analysis, producing the following threat products: Threat Activity Reports (TARs), Cyber Targeting Analysis Reports (CTARs), and CRF Supplements. This branch deep dives specific campaigns, actors, targeted technology, or a specific DIB incident to provide salient threat information and accompanying mitigation strategies.

Expanded Offerings and Projects (XOP) Division: XOP researches and provisions services and capabilities to support DIB Partners in protecting DoD information. These services are offered as pilots to the DIB Partnership, and encompass a wide range of cybersecurity concepts, technologies, and processes. XOP was created to provide evolving solutions based on the ever-changing cybersecurity environment and the diverse composition of the DIB partnership. Three branches constitute XOP:

1. **Assess Branch:** performs analysis of cybersecurity processes of DIB partners through the Cyber Resilience Analysis (CRA) tool. This branch also evaluates other vulnerability and penetration testing assessment procedures and provides them as a service to the DIB Partnership.

2. **Assist Branch:** evaluates cybersecurity technologies that can be provided to the DIB partnership as pilot programs. Cyber threat information gathered from such pilot programs is provided to the AD to analyze and include in information products to be disseminated to the DIB. Once a pilot is completed, if it is determined to be successful, it may be considered as a permanent service offering for the Partnership.

3. **Architect Branch:** researches and identifies the most effective ways to communicate with the DIB partnership. This research allows for informed recommendations for technologies that can best support rapid cyber threat information sharing between DoD and the DIB the Partnership.

Mission Support Division (MSD): The MSD functions in a number of areas, including providing services to internal and external customers, conducting outreach, compiling operational metrics, process improvement, quality assurance, quality control, and coordinating organizational training. MSD builds and manages relationships with a wide range of DIB companies and USG stakeholders, and drives special projects that improve the overall customer experience. MSD is comprised of two branches:

1. **Customer Engagement:** focused on building strong customer relationships to support the needs of the DIB, assists with onboarding and training for new DIB Partners; curates events, such as Technical Exchanges, Regional Partner Exchanges, web conferences, and panel discussions; and facilitates Analyst-to-Analyst, Business-to-Business, and Government-to-Government Exchanges.

2. **Organizational Readiness:** a team of knowledge managers, business and process analysts, quality control analysts, quality assurance analysts, training managers, process owners, and support staff who drive continual process improvement; systematically coordinates and aligns resources and functions in line with the vision, mission, goals and objectives of the DCISE Long Range Plan.

Pub. Date 4 JAN 2023