A FEDERAL CYBER CENTER

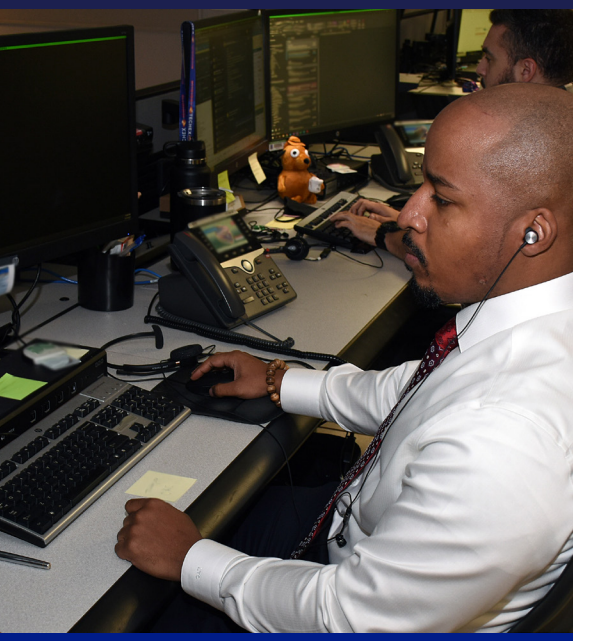
DoD CYBER CRIME CENTER

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

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE)–DCISE, the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program, safeguards intellectual property and DoD content on unclassified contractor networks. It facilitates public-private cyber threat information sharing, offers no-cost Cybersecurity-as-a-Service capabilities, and collaboration events with government/industry collaboration events. DC3 DCISE provides threat analysis, mitigation strategies, best practices, and exchanges for DIB participants of all sizes.

DC3 DCISE is the designated recipient for reporting DIB cyber incident reports as required by 10 U.S. Code Sections 391 and 393 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. While reports under the DFARS clause are mandatory, additional cyber DIB activity is reported on a voluntary basis.

- Collaborative partnership with over 1,100 Defense Contractors (DC) and US Government (USG) agency stakeholders
- Distributes a substantial number of actionable, non-attributable indicators daily
- Offers no-cost forensics, malware analysis, and cybersecurity services for DIB Partners
- Shares a significant number of cyber threat reports (hundreds annually) for both DIB and USG consumption (DIB Partners may access DC3 DCISE reporting via their DIBNET accounts and USG members can access via SIPRNet Intelshare)
- Operates 24/7/365 DC3 DCISE support hotline (1-877-838-2174) to assist submitters and DIB and USG Partners
- Rated as Capability Maturity Model Integration for Services (CMMI-SVC) Maturity Level 3



DCISE provides cyber resilience analyses for Defense Contractor (DC) companies, and offers unmatched Cybersecurity-as-a-Service capabilities.

DCISE CAPABILITIES

DC3 DCISE specializes in cyber activity analysis to understand cyber threats to unclassified DoD information on DIB systems and networks. This includes daily incident report processing, malware analysis, and engagement with partners to gather necessary information. Additionally, it conducts mid- to long-term analysis, producing threat reports and analyses for the DIB, including sharing downgraded classified information. DC3 DCISE produces technical analysis products and collaborates with USG agencies to ensure a whole-of-government approach to DIB cyber threats.

DC3 DCISE researches and provides cybersecurity services to DIB Partners, adapting to the evolving cybersecurity landscape. This involves evaluating cybersecurity resilience, performing vulnerability testing for DIB partners, and evaluating cybersecurity technologies through pilots. Insights from these activities are shared to facilitate rapid cyber threat exchange between DoD and the DIB Partnership.

DC3 DCISE handles DIB Partner services, outreach, metrics, and process improvement. We value strong customer relationships supported by user-friendly onboarding, information sharing events, and 24/7 responsiveness. Our team coordinates resources and functions to align with long-term plans, driving continual process improvement.

Oversees a collaborative partnership with over

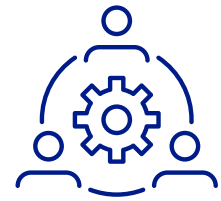
1,100

DCs and U.S. Government (USG) agencies

Disseminated over

15,000

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)



Provided more than

79,000

hours of no-cost forensics and malware analysis for DIB Partners