A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

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

DC3 DIB COLLABORATION

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

DoDD 5505.13e and DODI 5205.13 establish DC3 as the operational focal point for threat information sharing through the DCISE to protect unclassified DoD information residing on, or transiting Defense Industrial Base (DIB) unclassified networks.

DCISE and the DIBNet-U portal are the entry points for both mandatory (DFARS) and voluntary reporting under the DIB Cybersecurity (CS) Program. DCISE develops and shares actionable threat products, and performs cyber analysis, diagnostics, and remediation consults for DIB Partners as directed by DoDI 5205.13. DCISE collaborates with other DC3 directorates to include the Cyber Forensics Laboratory, Operations Enablement/Analytic Group, Technical Solution Development, and the Vulnerability Disclosure Program to provide strategic, operational, and tactical situational awareness to increase the DIB's ability to safeguard CUI data on information systems. 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.

(U) DIB CS Program

The 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 with participants, the program is designed to improve DIB network defenses, reduce damage to critical programs, and increase cyber situational awareness. DIB CS Program provisions and requirements are outlined in 32 CFR Part 236.

(U) 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

(U) Value of Participation

- Collaborative partnership with over 885 CDCs and USG agencies
- Engagement opportunities at many levels between USG and DIB, from C-suite to analyst level
- Access to indicator and threat products created from DIB reporting, multiple USG data streams, and industry cyber threat reports
- ~500,000 actionable, non-attributable (to submitting source) indicators
- ~78,000+ hours of no-cost forensics and malware analysis for Partners
- ~12,200+ cyber threat reports

(U) Threat Products

- Voluntary DIB Partner and mandated DFARS reporting are used to create threat products providing situational awareness and context of cyber activity. Products include:
  - Threat Activity Reports (TARs) focus on specific APT sets, campaigns, or malware
  - Cyber Targeting Analysis Reports (CTARs) focus on specific technology targeted by APT sets, campaigns, or malware
  - The Customer Response Form (CRF) Rollup and CRF Supplement enrich DIB mandatory and voluntary reporting to DCISE by providing actionable indicators and relevant context regarding cyber threat actor TTPs and targeting
  - Alerts/Warnings/Advisories provide information of importance to DIB Partners with the potential for effects due to possible breaches of network security measures
- Reports are available to DIB Partners via DIBNet and to USG via NIPR (https://intelshare.intelink.gov/sites/dodcc/dcise/default.aspx) and SIPR Intelshare (https://intelshare.intelink.sgov.gov/sites/dodcc/dcise/default.aspx

Pub Date: 23 May 2022

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center

(U) DFARS Mandatory Reporting

DoD contractors are required to report cyber incidents under the Defense Federal Acquisition Regulation Supplement (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 DFARS 252.204-7012 requirements and where to access additional information.

(U) Mandatory Incident Reporting Requirements

Mandatory incident reporting under DFARS 252.204-7012 is required by most DoD contracts and in subcontracts that involve CDI and/or operationally critical support programs involving CDI. Contractors must report the discovery of cyber incidents that affect CDI information systems, or the CDI information residing therein, to https://dibnet.dod.mil within 72 hours. Malicious software, affected system images, packet capture, and other data relevant to the reported cyber incident must be preserved for 90 days to allow time for DoD to request the data to conduct a damage assessment or decline interest.

(U) DC3/DCISE Notification Requirements

DC3 is designated by DFARS 252-204-7012 as the DoD focal point for receiving initial DIB cyber incident reports. PGI 204.73 requires DC3 to provide a copy of the mandatory incident report to contracting officer(s) for potentially impacted contracts identified in the report. DC3 is also required to notify various USG stakeholders dependent on circumstances. DCISE provides email notification of mandatory reporting to the DoD Damage Assessment Management Office, DIB CS PMO, DC3 Director, and the Joint Acquisition Protection and Exploitation Cell (JAPEC). Copies of mandatory incident reports are available within two hours of receipt for USG consumption on DCISE's SIPR Intelshare page at https://intelshare.intelink.sgov.gov/sites/dodcc/dcise/default.aspx.

After cyber incidents are reported via DIBNet, malicious software in connection with the incident is submitted to DC3 in accordance with instructions provided by DC3 or the Contracting Officer (KO). Attributional/proprietary information may only be released to entities with mission affected by such information; entities involved in the diagnosis, detection, or mitigation of cyber incidents; USG entities that conduct counterintelligence or law enforcement investigations; and for national security purposes.

(U//FOUO) Cyber Incident Notification (CIN) Reporting Requirements

A memo released by the Office of the Deputy Secretary of Defense on 4 May 19 titled, *"Defense Industrial Base Cyber Incident Notification Process,"* (also referred to as the Norquist Memo) establishes reporting requirements for notifying key DoD stakeholders of cyber incidents involving DIB contractors. The memo requires that DC3 create a Cyber Incident Notification (CIN) within three business days of discovery of a cyber incident involving significant loss of DoD PII, classified, and/or CUI information. CINs are sent via email notification to any applicable organizations which may include the National Joint Operations Intelligence Center, Defense Counterintelligence and Security Agency, Under Secretary of Defense for Intelligence, MDCOs, Contracting Officers in military departments, agencies, and combatant commands, OSD DAMO, DoD Chief Information Officer, OSD Chief Management Office. CINs are posted to the DCISE SIPRNet Intelshare page.

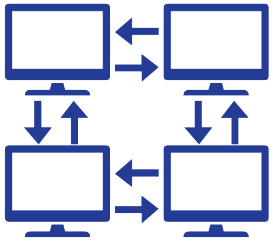
(U) What Does DCISE do with Mandatory Reporting?

DCISE analysts conduct outreach with submitting companies within three business days of their mandatory incident report submission to obtain relevant information regarding the reported incident; aid the submitting company with any malware submissions; and assist in the coordination of media submission requirements when DoD elects to conduct a damage assessment. DCISE analysts conduct multi-source research, with an emphasis on open internet research, to produce the CRF Rollup and CRF Supplements. These products are published to DIBNet and the Intelshare in support of the DIB CS Program and are sanitized of any attributional information. DCISE also shares information with DC3's Analytical Group, who generates Intelligence Information Reports (IIRs) and Cyber Intelligence Reports (CIR) for USG and the US Intelligence Community's consumption. Mandatory reporting may also be used in the development of various DCISE threat products, to include: TARs, CTARs, Alerts, Warnings, Advisories, and trend reports.

Learn more about DFARS 252.204-7012 at http://www. acq.osd.mil/dpap

Contractors report mandatory cyber incidents to the DIBNet portal at https://dibnet.dod. mil/portal/

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



DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center