DoD-DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE)

DoD-DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE)

Designated as the single focal point and data repository for Defense Industrial Base (DIB) cyber incident reporting, as required by 10 U.S. Code Sections 391 and 393 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, the Department of Defense (DoD) Cyber Crime Center (DC3) DIB Collaborative Information Sharing Environment (DCISE) enriches DIB reporting with all-source intelligence analysis and disseminates this information via various intelligence products, reports, and actor profiles to enable a broad range of actions against malicious cyber actors. While reports under the DFARS clause are mandatory, additional DIB cyber activity can be reported on a voluntary basis. Voluntary reporting enables DoW and the DIB to generate insights than enable cyber action.

- Collaborative partnership with over 1,100 Defense Contractors (DCs) and U.S. Government (USG) agency stakeholders
- Daily publication of actionable, relevant, and timely cyber threat indicators
- Offers forensics, malware analysis, and cybersecurity capabilities for DIB Partners
- Shares a significant number of cyber threat reports (hundreds annually) for both DIB and USG consumption (USG members can access via SIPRNet Intelshare)
- Operates 24/7/365 DC3 DCISE support hotline (1-877-838-2174) to assist with incident reporting for DIB and USG Partners
- Rated at Capability Maturity Model Integration for Services (CMMI-SVC) Maturity Level 3

DCISE THREAT PRODUCTS

DCISE produces products ranging from indicator based to strategic cyber threat analyses.

Voluntary DIB Partner and mandated DFARS reporting are used to create threat products providing situational awareness and context of cyber activity. Products include the following:

- **Threat Activity Reports (TARs)** focus on specific APT sets, campaigns, or malware.
- **Cyber Targeting Analysis Reports (CTARs)** focus on specific technology targeted by Advanced Persistent Threat (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 tactics, techniques, and procedures (TTPs) and targeting.
- **Alerts/Warnings/Advisories** provide the DIB with timely information regarding zero-day and other actively exploited vulnerabilities, critical vulnerabilities, APT activity, and adversarial TTPs.
- The **TIPPER** alerts Partners via email about imminent or recent suspicious cyber activities and vulnerabilities specific to the DIB Partner.
- The **Threat Information Product (TIP)** contains Controlled Unclassified Information or Unclassified indicators from multiple sources.
- The **Weekly Indicator Roundup (WIR)** provides Partners with a regular gathering of indicators, eliminating the need to compile indicators from separate sources. This enables Partners to automatically ingest indicators into their security appliance.

PROGRAM POLICY-RELATED RESOURCES

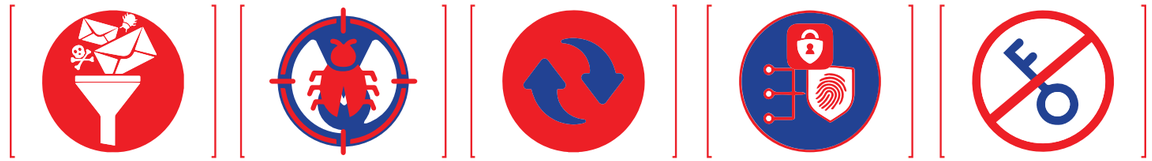
Please visit **dc3.mil** for links to the following:

- 32 Code of Federal Regulations Part 236, DoD's DIB Cybersecurity Activities
- Title 48 of the Code of Federal Regulations
- DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"
- DFARS 252.239-7010 "Cloud Computing Services"
- Federal Acquisition Regulation (FAR) 52.204-23 "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities"
- FAR 52.204-25 "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment"

DCISE'S TOP 5 MITIGATION TIPS

1. **Patching:** Conduct routine scanning and ensure all software and services are up-to-date.
2. **Insecure Default Configurations:** Ensure that all default configurations are promptly changed and secured.
3. **Spearphishing Weakness:** Deploy email filtering and/or scanning.
4. **Spearphishing Susceptibility:** Conduct user training.
5. **Unnecessary Network Solutions:** Disable any network solution that is not being utilized to make the attack vector smaller.

DCISE RECOMMENDED TOP 5 CYBERSECURITY PRACTICES



DC3 DIB COLLABORATION

DFARS Mandatory Reporting

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

Mandatory incident reporting under DFARS 252.204-7012 is required by most DoW 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, within 72 hours. Affected system images, packet capture, and other data relevant to the reported cyber incident must be preserved for 90 days to allow time for DoW to request the data to conduct a damage assessment or decline interest.

DCISE Notification Requirements

DC3 is designated by DFARS 252-204-7012 as the DoW focal point for receiving initial DIB cyber incident reports. Procedures, Guidance, and Information (PGI) 204.73 requires DC3 to provide a copy of the Mandatory Incident Report (MIR) 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 DoW Damage Assessment Management Office (DAMO), DIB CS PMO, DC3 Director, and the Joint Acquisition Protection and Exploitation Cell (JAPEC). Copies of MIRs 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. Attributional/proprietary information may only be released to entities with missions 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.

What is DCISE's Role in Mandatory Incident Reporting?

DCISE receives and processes MIRs from DIB Companies (DIBCOs). DCISE analysts routinely perform the following tasks:

- Conduct outreach with submitting companies to obtain relevant information regarding the reported incident.
- Assist the submitting company with any malware submissions.
- Assist in coordinating media submission requirements when DoW elects to conduct a damage assessment.
- Coordinate and deconflict with other DoW and USG entities, such as law enforcement or counterintelligence, that may already be investigating the incident. This helps ensure DIBCOs are not burdened by multiple USG entities asking for similar information.

What Does DCISE Do With the Information Provided?

The incident details provided to DCISE by a DIBCO in the ICF are used to support the cybersecurity posture of the DIB. DCISE does this by generating threat intelligence products that are shared with DIB Partners. The threat intelligence products are non-attributable, which means the identity of the submitting company is never revealed. The threat intelligence products range from incident-level analyses to strategic-level reports on which technologies are being targeted by state-sponsored cyber actors. The information a DIBCO provides can also assist in sanctions or arrests of cyber-criminals and adversarial nations. The MIR ICF is also shared with other USG agencies.

Common Misunderstandings About Mandatory Incident Reporting

Media and Malware Submissions

While it is important to work with law enforcement agencies—such as the Federal Bureau of Investigation—on cyber-related crimes, providing forensic images and third-party forensic reports to a Department of Justice entity does not fulfill the DFARS requirement to the DoW.

Ways to Report:

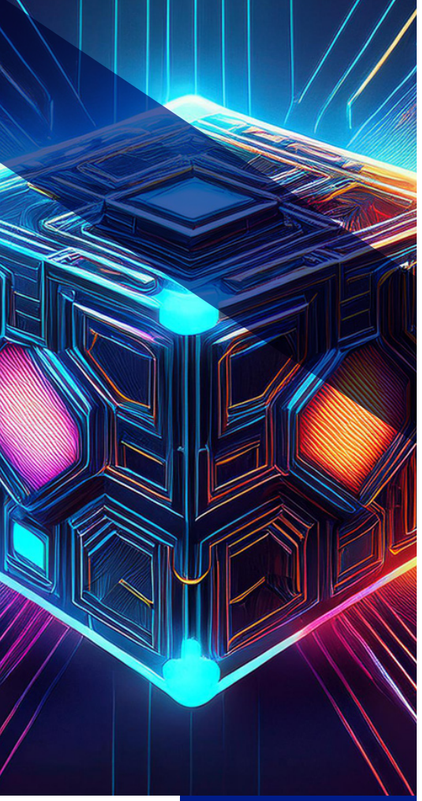
- The preferred method to report cyber incidents is to acquire a DoW-approved medium assurance certificate, which enables the timely and protected transfer of incident details to DCISE.
- **DoD SAFE:** Partners will contact DCISE to receive a DoD Secure Access File Exchange (SAFE) password that will expire after 72 hours. The DIBCO will complete the necessary documents, and our analysts will report on the Partner's behalf.

Third-Party Forensic Reports

DCISE will request Partners to submit third-party forensic reports as they become available. In the event of an incident where a DIB company engages a third-party forensic firm for investigation, DCISE will ask for a copy of the report for further analysis and collaboration.

DCISE EVENTS

- **Partner Familiarization Event (PFE):** Introductory meeting between DCISE and newly onboarded DIB Partners. Discussions include DCISE and Partner Points of Contact (POCs) and submission incident reports.
- **Analyst-to-Analyst (A2A) Exchanges:** DIB Partner-driven and may address APT TTPs, technology targeting, and current threat reporting. Opportunity for one-on-one diagnostics and remediation with DCISE analysts.
- **Business-to-Business (B2B)** Exchanges: Introduction to DCISE products and services to DIB POCs and their corporate leadership in addition to highlighting the positive business impact of network security.
- **DC3 Technical Exchange (TechEx):** Bi-annual meetings between DIB Partners and USG stakeholders to share best practices, threat briefs, lessons learned, tools, and other industry insights at classified and unclassified levels.
- **Regional Partner Exchange (RPEX):** Provides an opportunity for local DIB Partners within the same geographic region to have a TechEx experience on a smaller scale. DCISE leadership and analysts provide a tailored threat brief covering the current threat landscape, specific APT trends, and threat actor TTPs. Partners have the opportunity to network, discuss topics of concern, present briefs, chair panels, and collaborate.
- **DCISE F.I.R.E.:** One-day, technology-supported table top exercise event led by DCISE (in-person or remote) for DIB Partners to test their skills in a variety of topics (e.g., incident response, intrusion detection) while earning Continuing Professional Education credits.
- **DIB Webinar:** DCISE provides a platform for DIB Partners and DCISE analysts to engage in classified, detailed discussions on adversary techniques and trends. These sessions aren't limited to just technical topics; they also cover a broad spectrum of issues relevant to the DIB, led by various experts from DCISE.



DCISE³ AT A GLANCE

DCISE recognizes the unique challenges faced by the small and medium businesses within the collective DIB and has partnered with Celerium to provide an automated cyber threat detection, scoring, and blocking solution to our DIB CS Program participants.

How Does It Work?

DCISE³ integrates with a company's existing firewall and captures a real-time stream of metadata associated with network traffic that contains the IP address and domains with which communications are occurring.

DCISE³ automatically aggregates this metadata and provides fully automated risk-scoring capabilities for every network connection without requiring any human interaction. Risk scoring takes into account over 60 sources of threat intelligence (including DCISE indicators), years of historical data, and predictive algorithms to detect and automatically block emerging and pre-existing threats.

This offering has been upgraded to DCISE³ v2 as of August 2024 and now offers enhanced network reporting, an updated user interface, and expands the network defense orientation of v1 to data breach defense and other additional features. The upgraded solution was tested with DIB CS members that found the new version to be easier to use and provide additional value.

Network Defense Functions

- Port threat activity reports
- Network threat activity reports
- 24-hour network threat reports
- Live network threat data reports
- Optional automated blocking of malicious network traffic
- Re-optimization of network blocklist every 15 minutes per firewall
- Blocking activity—receive notification anytime an IP address is blocked

Data Breach Defense Functions

- Track potential data breach activity
- Enable manual activation of containment via blocking

Malware Defense Functions

- Detect and optionally block selected malware activity (Volt Typhoon, MOVEit, TrueBot, and others)

Implementation

DCISE³ v2 is engineered to support companies with overloaded and overwhelmed IT organizations and can be implemented without needing installation of any hardware or software. The implementation is based on configuring public-facing firewalls in 30 minutes or less. The solution is minimally intrusive, meaning it does not access any customer data or packets since it focuses on Layer 3 syslog meta data.

ALL-TIME PROGRAM METRICS

3.8M
Threats Detected

1.8M
Threats Blocked

WE PROVIDE

Federal Compliance | Real-time Visibility | Traffic Analysis | Auto Blocking

DC3 PROGRAM OFFERINGS

DIB–VULNERABILITY DISCLOSURE PROGRAM (DIB–VDP)

DC3 and Defense Counterintelligence and Security Agency (DCSA) have established a fully operational vulnerability disclosure program supporting the DIB. DC3's DIB-VDP performs a coordinated vulnerability disclosure process of ingesting information from designated vulnerability researchers. The information is then shared with relevant stakeholders to ensure timely remediation. Once vulnerabilities are validated, DC3 uses non-attributed disclosures to communicate both the vulnerabilities and their mitigations. Leveraging this proven model is the most effective way to encourage vulnerability discovery within DIBCOs' publicly accessible information systems.

Each mitigated vulnerability saves the affected company an average of ***$10.2m*** *in response and recovery costs.*

Source: https://www.ibm.com/reports/data-breach

ENHANCED NETWORK SENSOR AND INTELLIGENT THREAT ENUMERATION (ENSITE)

The ENSITE program is a comprehensive cybersecurity solution accessible to the DIB, offering robust protection with continuous, real-time monitoring, advanced AI/ML-powered threat detection, and tailored support from DC3 analysts. Key features include a centralized dashboard, integration with the MITRE ATT&CK framework and support for meeting NIST 800-171 security objectives.

MALWARE AND FORENSIC ANALYSIS

DCISE is your point of contact for submitting malware and/or other relevant files to the DC3 Cyber Forensics Laboratory (CFL) for a quick triage or an in-depth examination and can be submitted as part of a Voluntary or Mandatory ICF submission.

Ways to Submit Malware to DC3 CFL:

- Traditional mail
- DC3 Electronic Malware Submission (EMS) portal (**https://ems.dc3on.gov/**)
  - Application Programming Interface (API) available to upload malware and retrieve analysis results
  - Email service account available for fast upload of suspicious emails
- **DO NOT email malware to anyone at DCISE**

AUTOMATED MALWARE RESPONSE (AMR)

The DC3 EMS portal provides an option for AMR. This capability provides the following:

- A quick, automated analysis of your submitted malware, phishing emails, email attachments, or other suspicious files
- Results ready in less than 15 minutes
- Results that include antivirus engine checks, file attributes, notable strings, YARA signature matches, and more

DoD CYBER CRIME CENTER

410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

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

𝕏 @DC3Forensics 𝕏 @DC3DCISE

DC3 Cyber Crime Center