A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

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

DoD'S DIB CS PROGRAM

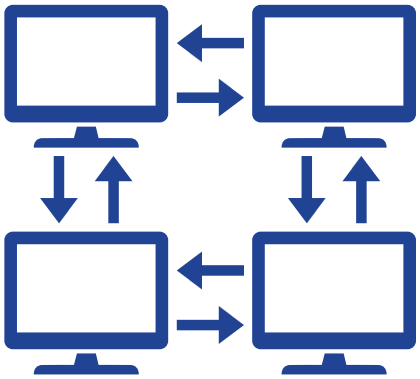
Contact Information

DCISE:

- DC3.DCISE@us.af.mil
- DCISE Hotline (410) 981-0104

DIB CS Program Management Office:

- OSD.DIBCSIA@mail.mil



DC3/DCISE Service Offerings

DC3/DCISE offers many Cybersecurity-as-a-Service (CaaS) products at no cost to DIB CS Partners:

- **Cyber Resilience Analysis (CRA):** evaluates processes and practices across 10-security domains that provides insight into an organization's operational resilience and ability to manage cyber attacks
- **DCISE³:** deploys instantly and delivers enterprise-grade threat identification and real-time monitoring of your network
- **Krystal Ball (KB):** maps public-facing infrastructure and overlays it with threat-intelligence sources
- **Adversary Emulation (AE):** conducts penetration testing, which includes network mapping, vulnerability scanning, phishing assessments, and web application testing. Adversary Emulation merges technical, process, and policy issues into a single, actionable framework

Common Acronyms

- Advanced Persistent Threat (APT)
- Analyst-to-Analyst (A2A)
- Business-to-Business (B2B)
- Cyber Resilience Analysis (CRA)
- Customer Response Form (CRF)
- Cybersecurity (CS)
- Cyber Targeting Analysis Report (CTAR)
- DoD Cyber Crime Center (DC3)
- DoD-DIB Collaborative Information Sharing Environment (DCISE)
- Defense Industrial Base (DIB)
- Electronic Malware Submission (EMS)
- Government-to-Government (G2G)
- Incident Collection Format (ICF)
- Mandatory Incident Report (MIR)
- Partner Familiarization Event (PFE)
- Point of Contact (POC)
- Policy and Operations Working Group (POWG)
- Public Key Infrastructure (PKI)
- Regional Partner Exchange (RPEX)
- Request for Information (RFI)
- Threat Activity Report (TAR)
- Threat Information Product (TIP)
- Tactics, Techniques, and Procedures (TTP)
- Technical Exchange (TechEx)
- Technology and Architecture Working Group (TAWG)
- Virtual Industry-Based Partner Exchange (VIPEX)
- Weekly Indicator Round-Up (WIR)

DoD'S DIB CS PROGRAM

Program Policy Related Resources

- 32 Code of Federal Regulations (CFR) Part 236, DoD's DIB Cybersecurity Activities
  https://www.federalregister.gov/documents/2016/10/04/2016-23968/department-of-defense-dods-defense-industrial-base-dib-cybersecurity-cs-activities
- DFARS 252.204-7012 *"Safeguarding Covered Defense Information and Cyber Incident Reporting"*
  https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
- DFARS 252.239-7010 *"Cloud Computing Services"*
  https://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7010
- FAR 52.204-23 *"Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities"*
  https://www.acquisition.gov/far/52.204-23
- FAR 52.204-25 "*Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment"*
  https://www.acquisition.gov/far/52.204-25

DIBNet-U Portal https://dibnet.dod.mil/

The DIBNet-U Portal is DoD's gateway for defense contractor cyber incident reporting and participation in the DoD-DIB CS Program. The DIBNet-U Portal's splash page is home to various DC3/DCISE offerings.

Navigate to the DIBNet-U splash page to learn more about:

- The Cyber Threat Roundup (CTR): a collection of recent open-source articles of interest for the DIB
- DCISE-Recommended Top Five Cybersecurity Practices for small and medium companies
- DIB-Reported Cyber Threats

DIBNet User Types (Company Representative, Technical POC, or Regular User)

Value of being the Company Representative:

- Responsible for nominating additional DIBNet users
- Responsible for keeping Company POC up to date
- Primary POC for DIB Communications

Value of being a Technical POC:

- Receives ALL DCISE encrypted communications, including Participant Reports
- Real-time awareness of DIB-reported activity

DIBNet-U Regular User:

- Access to DIBNet-U including:
  - Reporting
  - Forums
  - Presentation Slides
- Time-sensitive Alerts & Warnings
- Designated to share cyber activity via ICF with DCISE
- Invitations to DCISE-led events

DoD'S DIB CS PROGRAM

DC3/DCISE Events

DC3/DCISE facilitates a number of events throughout the year. Registration for events is done through the Customer Portal (https://customerportal.dc3.mil). If you have issues registering for an event, email **DC3.DCISE@us.af.mil** and our team can help.

- **PFE:** Introductory meeting between DC3/DCISE and newly onboarded DIB CS Program Partners. Meeting discussions include the role of DC3/DCISE and Partnership member participation, overview of offerings available, and cyber activity/incident reporting guidance.
- **TechEx:** Semi-annual meetings between DIB Partners and USG stakeholders to share best practices, lessons learned, tools, and other industry insights.
- **RPEX:** Provides an opportunity for local DIB Partners within the same geographic region to have a TechEx experience on a smaller scale. DC3/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.
- **VIPEX:** Virtual counterpart to the RPEX, with a tailored threat briefing, opportunities for networking, and small group discussions. Event attendance is determined by industry, sector, company size or other significant factors, vice solely by geographic region.
- **A2A:** DIB Partner-driven and may address APT TTPs, technology targeting, and current threat reporting.
- **B2B:** Introduction to DCISE products and services to DIB POCs and their corporate leadership in addition to highlighting the positive business impact of network security and participation in the DIB CS Program.
- **G2G:** Conducted between government colleagues and DC3 analysts and/or Leadership. These meetings may follow the format of an A2A, B2B, or simply provide an opportunity to share, collaborate, and discuss.
- **DIB Web Conference/DIB Teleconference:** Enable DIB Partners and DCISE analysts to have unclassified, granular and technical discussions on adversary techniques and trends. DCISE schedules a recurring series of introductory web conferences called "Partner Essentials." Partner Essentials web conferences are tailored to assist new Partners, new Partner POCs, and others to fully acclimate to the DIB CS Program. In addition, DCISE provides the Partnership with video presentations that are hosted online for training purposes. These offerings may or may not be monitored and offer the flexibility to view the latest educational recordings that DCISE has to offer.

DC3/DCISE Analytics Division (AD) Products

DC3/DCISE produces products ranging from indicator-based to strategic cyber threat analyses

- **DC3/DCISE Threat Reporting:**
  - **TIP:** Derived from USG reporting; includes relevant IOCs to DIB/CDCs and narrative context
  - **CRF Rollup/Supplement:**
    - CRF Rollup – Derived from DIB reporting; includes relevant IOCs to DIB/CDCs and narrative context
    - CRF Supplement – Produced when additional amplifying data becomes available after initially reported in CRF Rollup (i.e. malware samples)
  - **CTAR:** In-depth risk analysis product detailing adversarial cyber targeting of US DoD technology/ platforms/systems
  - **TAR:** In-depth analysis of cyber threat actors' TTPs against DIB targets

DoD'S DIB CS PROGRAM

- **DC3/DCISE Notifications:**
  - **Alerts**, **Warnings**, **Advisories**, **TIPPERs**
  - Vehicles to notify DIB Partners of varying levels of cyber threats (critical through situational)
- **DC3/DCISE Informational Reporting:**
  - **WIR:** Roundup of DCISE IOCs released in DCISE products for the given week
  - **Cyber Threat Round-Up:** Compilation of relevant cyber news articles, posted to DIBNET splash page
  - Slick Sheets (on varying topics)

Mandatory vs Voluntary Reporting

Mandatory

- DFARS 252.204-7012 – Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting
- Cyber incident that affects:
  - CDI and/or the systems it resides on, or
  - Ability to provide operationally critical support

Voluntary

- Helps DIB with situational awareness and indicator sharing
- Crowdsourcing threat information
- Types of events vary
- No impact to DoD information

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 - for free
- Can be submitted as part of a Voluntary or Mandatory ICF submission

Ways to Submit to DC3 CFL

- Traditional Mail
- DC3 Electronic Malware Submission (EMS) Portal (https://ems.dc3on.gov/)
  - Can also be accessed directly through DIBNet-U
- DoD SAFE (Secure Access File Exchange) https://safe.apps.mil
- **Please do not email malware to anyone at DC3/DCISE**

Automated Malware Response (AMR)

- The DC3 Electronic Malware Submission (EMS) portal provides an option for Automated Malware Response (AMR). This capability provides:
  - Completes a quick, automated analysis of your submitted malware, phishing emails, email attachments, or other suspicious files
  - Results ready in less than 15 minutes
  - Results include antivirus engine checks, file attributes, notable strings, YARA signature matches, and more

DIB CS Program & DC3/DCISE Videos

Watch the DIB Tech Talk Interview Series for an in-depth overview of the DoD's DIB CS Program & DC3:

- **In-Depth Look at DoD's DIB CS Program** - https://www.youtube.com/watch?v=kIsJph_szCY
- **Meet DoD's DC3/DCISE** - https://www.youtube.com/watch?v=vb9fTKh5Cxg
- **Meet DoD's Vulnerability Disclosure Program (VDP) -** https://www.youtube.com/watch?v=wMUREvjvZeA

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

DoD'S DIB CS PROGRAM

FAQs

Q: How do I reactivate my DIBNet-U account?
A: Email DC3.DCISE@us.af.mil with your request and our Customer Engagement team will work with you on reactivation.

Q: How do I become a POC?
A: To become a POC, send an email to DC3.DCISE@us.af.mil and include your name, email address, and phone number.

POCs are required to have the following:

- DoD-approved medium assurance certificate (see https://public.cyber.mil/eca/ for details)
- Signed Non-Disclosure Agreement

Q: How often should I login to DIBNet-U to keep my account active?
A: Login to your account at least once every thirty five (35) days or your account will automatically deactivate.

Q: My cert on file has expired. How can I update my DIBNet-U account?
A: Email DC3.DCISE@us.af.mil and request a recertification link be sent to you by a member of the Customer Engagement team.

Q: Can I follow DC3/DCISE on social media?
A: Twitter: https://twitter.com/DC3DCISE
LinkedIn: https://www.linkedin.com/company/defense-cyber-crime-center/

Q: How do I nominate other personnel from my company for a DIBNet-U account?
A: If you are the Company Representative you may nominate other personnel from your company by logging into DIBNet-U and selecting "User Nomination" from the left-side navigation. The nominated user will need to complete an NDA, have an approved medium assurance certificate, and complete all account registration requirements in order to be approved. You may also email DC3.DCISE@us.af.mil with your request (including nominee's name, email address, phone number, permission type), and we will be happy to submit the nominate request on your behalf.

Q: How do I submit a Mandatory Report/Voluntary Report?
A: All Mandatory/Voluntary Reports can be submitted through the DIBNet-U (https://dibnet.dod.mil) splash page. You may also call the DCISE Hotline to report an incident (410) 981-0104.

Q: I am departing my company and I am the only POC listed. What should I do?
A: Please keep DC3/DCISE updated on all personnel moves. If there is a POC change within your company, please email DC3.DCISE@us.af.mil with a listing of who will be the new designated POC for your company so that we may get that individual nominated for a DIBNet-U account.

Q: How do I register for a Customer Portal account?
A: Navigate to DC3 Customer Portal (https://customerportal.dc3.mil) and authenticate with your approved medium assurance certificate. Request an account and then request access to the DCISE Events space (be sure not to check the box for "I already have an account"). The Customer Engagement team will approve your request shortly.

Additional Questions?
Contact us now (410) 981-0104

Pub Date: 2 Aug 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