DoD's Defense Industrial Base Cybersecurity Program

Mission: Enhance and supplement Defense Industrial Base (DIB) Program participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified information systems.

Launched In:
2008

Who Are We?

A public-private cybersecurity partnership that provides a collaborative environment for sharing unclassified and classified cyber threat information.

What Do We Do?

Through the construct of the DIB Cybersecurity Program, cyber threat information is shared between DoD and the DIB, so that all parties have a near real-time picture of the current threat environment.
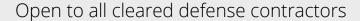
How Can We Help?

Information is shared bi-directionally between DoD and the DIB. DoD disseminates alerts and warnings to notify the DIB of critical, time-sensitive information through DIBNet.

Joining the DIB CS Program: Application Process

Step 1: Apply

Apply from https://dibnet.dod.mil using a DoD-approved medium assurance certificate

Free of cost

Open to all cleared defense contractors

Step 2: Verify

- DIB CS Program Management Office (PMO) verifies that the prospective participant:
  1. Has an existing active facility clearance (FCL)
  2. Has identified a Company Representative who is a U.S. Citizen and is authorized to act on behalf of the company
- If all eligibility requirements are met, the DIB CS PMO notifies the prospective participant that the Framework Agreement (FA), Amendments, and the non-disclosure agreement (NDA) are available for review and signature in DIBNet

Step 3: Sign

- Prospective participant returns the signed FA, Amendments (if applicable), and NDA
- DoD countersigns the FA and returns the signed agreement to the company
- Once the FA has been signed by the company and DoD, the information sharing relationship is finalized, and the company is now a participant in the DIB CS Program

Step 4: Welcome

- DIB CS PMO conducts an onboarding call to introduce the products and services offered in conjunction with the Program
- DIB CS participants' DIBNet accounts are fully-activated and they can engage with the DIB CS PMO and DoD Cyber Crime Center (DC3), to receive cyber threat information and participate in program-related engagements like working groups and DIBNet forums
- Additional information from USG components with DIB equities is shared on the platform