DoD's DIB Cybersecurity Program

Public – Private Cybersecurity Collaboration

The United States continues to face significant risk that malicious actors can compromise critical Defense information residing on Defense Industrial Base (DIB) networks and cause potential economic losses or damage to U.S. national security. The DIB develops and maintains sensitive technology and intellectual property vital to protecting and defending our nation. As a consequence, malicious cyber actors regularly target the DIB and look for ways to access company networks and obtain valuable information that may compromise our national security and warfighting capabilities.

The Department of Defense (DoD) established the DIB Cybersecurity (CS) program to enhance and supplement DIB participants' abilities to safeguard DoD information. Under the voluntary DIB CS program, DoD and DIB participants share cyber threat information in order to enhance the overall security of unclassified DIB networks, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness.

For more information about the DIB CS program see 32 Code of Federal Regulations part 236, "DoD-Defense Industrial Base Cybersecurity Activities" (https://www.federalregister.gov/articles/2015/10/02/2015-24296/department-of-defense-dod-defense-industrial-base-dib-cybersecurity-cs-activities). *

Cyber Threat Information Sharing

DIB participants are encouraged to report information and share cyber threat indicators that they believe are valuable in alerting the Government and others in order to better counter threat actor activity.

Through the program's operational focal point, the DoD Cyber Crime Center (DC3), DoD and DIB participants share unclassified and classified cyber threat information in near-real time and respond to adversary activity. Shared information includes mitigation measures and cybersecurity best practices that can help bolster DIB participants' cybersecurity posture. DC3 also analyzes malware and helps industry partners develop mitigation strategies.

DIB Company Participation

The DIB CS Program is open to all cleared defense contractors. The DIB CS program is built upon a strong trusting relationship between DoD and Industry participants. DoD preserves the integrity of the program by protecting sensitive non-public information from unauthorized use and disclosure.

Visit https://dibnet.dod.mil to learn more about or apply to join the DIB CS information sharing program. For more information please contact: OSD.DIBCSIA@mail.mil.

* The 32 CFR part 236 Final rule was published on Oct. 4, 2016 and can be found at https://www.gpo.gov/fdsys/pkg/FR-2016-10-04/pdf/2016-23968.pdf.