U.S. Department of Defense

DoD Defense Industrial Base Cybersecurity Services

The Department of Defense (DoD) recognizes the need to help Defense Industrial Base (DIB) organizations improve their cybersecurity posture and operational resilience and to help the DIB protect DoD information that resides on and transits DIB information systems. DoD provides free cybersecurity services and information to DIB organizations. A variety of services are available based on your organization's specific needs. All members of the DIB community are eligible to participate. Visit the websites below or contact the DIB Cybersecurity (CS) Program at OSD.DIBCSIA@mail.mil for more information about cybersecurity training, services, and products.

DoD CYBER CRIME CENTER (DC3)

CATEGORIES	
✓ network traffic monitoring ✓ threat detection/ blocking	**DoD-DIB COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE) CUBED:** DCISE has partnered with a service provider to offer real-time monitoring of your organization's network traffic, threat detection, and alerts as well as the option to block malicious traffic. This service includes real-time network traffic monitoring for malicious sources and destinations at no cost and shares data anonymously. Malicious traffic is alerted on and, if desired, blocked. The service protects against distributed denial-of-service (DDoS) and domain name system (DNS) attacks.
✓ cybersecurity program evaluation	**CYBER RESILIENCY ANALYSIS (CRA):** Offers a structured review of an organization's cybersecurity posture with the goal of understanding cybersecurity capabilities and operational resilience and improving the ability to manage risk to critical services and assets. A structured survey conducted either in a DC3-facilitated session or as a self-assessment produces a report with suggested actions aligned with the 10 security domains that map to NIST SP 800-171 requirements to protect CUI and the NIST Cybersecurity Framework.
✓ network mapping ✓ vulnerability scanning ✓ phishing assessments	**ADVERSARY EMULATION (AE):** Analyzes an organization's vulnerability to threat actors based on network architecture, software, and processes. It includes technical, process, and policy evaluations in a single, actionable framework. AE may include penetration testing, network mapping, vulnerability scanning, phishing assessments, and web application testing. HTTPS://WWW.DC3.MIL or email DC3.INFORMATION@US.AF.MIL
✓ awareness ✓ risk assessment ✓ vulnerability scanning	**DIB-VDP:** A voluntary program for DIB companies that provides vulnerability discovery, triaging, and validation. DIB-VDP researchers facilitate timely vulnerability remediation by the system owner to reduce risk. Leveraging this proven model is the most effective way to encourage vulnerability discovery within DIB companies' publicly accessible information systems. Participation does not require DIB CS Program enrollment. HTTPS://WWW.DC3.MIL/MISSIONS/VULNERABILITY-DISCLOSURE or email AFOSI.DC3.DIB-VDP@US.AF.MIL

NATIONAL SECURITY AGENCY (NSA) CYBERSECURITY COLLABORATION CENTER (CCC)

✓ network traffic monitoring ✓ threat detection and blocking	**PROTECTIVE DOMAIN NAME SYSTEM (PDNS+):** Combines commercial cyber threat feeds with the NSA's unique insights to filter external DNS queries and block known malicious or suspicious website traffic, mitigating nation-state malware, spearphishing, botnets, and more.
✓ asset discovery ✓ vulnerability scanning	**ATTACK SURFACE MANAGEMENT:** Helps DIB customers find and fix issues before they become compromises by identifying internet-facing assets, then leveraging commercial scanning services to find vulnerabilities or misconfigurations on these networks. Each customer receives a tailored report with issues to remediate, prioritized based on both severity of the vulnerability and whether or not it is being exploited.
✓ risk assessment ✓ security assessment ✓ system/ information integrity	**AUTONOMOUS PENETRATION TESTING:** Leverages AI to automate pen-testing, enabling DIB companies to identify and mitigate vulnerabilities within their internal networks. The service also provides visualizations, tailored mitigation guidance, and the ability to verify whether or not a DIB company has implemented the suggested mitigations effectively. HTTPS://WWW.NSA.GOV/CCC or email DIB_DEFENSE@CYBER.NSA.GOV

OFFICE OF SMALL BUSINESS PROGRAMS (OSBP) PROJECT SPECTRUM

✓ awareness ✓ training ✓ tools and services	**PROJECT SPECTRUM:** Offers a wide variety of services, including cybersecurity information, resources, tools, and training. Its mission is to improve cybersecurity readiness, resiliency, and compliance for small and medium-sized businesses and the federal manufacturing supply chain. Project Spectrum includes information about security, risk, and compliance assessments; readiness checks, training, reviews of tools, current research, and policy. Project Spectrum provides information about USG and commercial services and tools, both free and fee based. HTTPS://WWW.PROJECTSPECTRUM.IO/

For further information contact the DIB CS Program.

https://DIBNet.dod.mil
linkedin.com/in/dod-cio
OSD.DIBCSIA@mail.mil
@DoD_CIO