U.S. Department *of* Defense

# Department of Defense (DoD) Defense Industrial Base (DIB) **Cybersecurity-as-a-Service (CSaaS)** Services and Support

The DoD recognizes the need to help 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.

### What is this?

Free cybersecurity services and information provided by the DoD to DIB organizations

### Who is this for?

All members of the DIB

### How?

A variety of services are available based on your specific needs. Visit the websites below for information about cybersecurity training, services, and products. You may also contact the DIB CS PMO at **OSD.DIBCSIA@mail.mil** to request additional details about these services.

## DC3/DOD DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE)

*Eligibility: The DIB CS Program is open to cleared defense contractors. The DoD has proposed changes to the eligibility requirements outlined in 32 CFR part 236 that will expand the program to contractors that own or operate a covered contractor information system.*

### DCISE³

**CATEGORIES**

- network traffic monitoring
- threat detection and blocking

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 and shares data anonymously at no cost. Malicious traffic is alerted on and, if desired, blocked. The service protects against DDOS and DNS attacks.*

**https://www.dc3.mil** or email **DC3.Information@us.af.mil**

### CYBER RESILIENCE ANALYSIS (CRA)

**CATEGORY**

- cybersecurity program evaluation

This program 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 the NIST SP 800-171 requirements to protect CUI and the NIST Cybersecurity Framework.*

**https://www.dc3.mil** or email **DC3.Information@us.af.mil**

### ADVERSARY EMULATION (AE)

**CATEGORIES**

- network mapping
- vulnerability scanning
- phishing assessments

This program 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**

# DoD DIB CSaaS

## NATIONAL SECURITY AGENCY (NSA) CYBERSECURITY COLLABORATION CENTER

*Eligibility: Any company (prime or sub) with a DoD contract or access to non-public DoD information*

### PROTECTIVE DOMAIN NAME SYSTEM (PDNS)

**CATEGORIES**

- network traffic monitoring
- threat detection and blocking

The NSA's PDNS service 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.

**https://www.nsa.gov/CCC** or **DIB_Defense@cyber.nsa.gov**

### ATTACK SURFACE MANAGEMENT

**CATEGORIES**

- asset discovery
- vulnerability scanning

This service helps DIB customers find and fix issues before they become compromises by identifying DIB 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.

**https://www.nsa.gov/ccc** or **DIB_Defense@cyber.nsa.gov**

## PROJECT SPECTRUM

**CATEGORIES**

- awareness
- training
- tools
- services (both free and paid)

Sponsored by the DoD Office of Small Business Programs (OSBP), Project Spectrum offers a wide variety of services, including cybersecurity information, resources, tools, and training. Their 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 U.S. Government and commercial services and tools, both free and fee based.*

**https://www.projectspectrum.io/#/**

## BLUE CYBER INITIATIVE

**CATEGORIES**

- awareness
- training

The U.S. Air Force's Blue Cyber Education Series for Small Businesses provides free and open-to-the-public cybersecurity information and support.

*Participate in daily, weekly, and monthly cybersecurity online help sessions and webinars. Learn about state and federal resources and collaborate across the federal, academic, and national small business ecosystem. Explore links to other DoD-sponsored Small Business Innovation Research cybersecurity programs.*

**https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/**