



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 and 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/ccs> 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 Department of the Navy CISO'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/>



Securing Critical Supply Chains in the Defense Industrial Base (DIB)

Defense Industrial Base (DIB) companies are relentlessly targeted by our adversaries, who seek to steal U.S. intellectual property, sensitive DoD information and DIB proprietary information to undermine our national security advantage and economy. NSA is working to contest these efforts by providing no-cost cybersecurity services to qualifying DIB companies. NSA's services are designed to help protect sensitive, but unclassified, DoD information that resides on private sector networks by hardening the top exploitation vectors that foreign malicious actors are using to compromise networks.

Eradicating cybersecurity threats to the DIB is an NSA priority. NSA's Cybersecurity Collaboration Center (CCC) provides no-cost cybersecurity solutions for qualifying DIB companies. These solutions are easily implemented and scalable to protect against the most common nation-state exploitation vectors and are designed to help protect DoD information and reduce the risk of compromise. These services include Protective DNS, attack surface management, and access to NSA non-public, DIB-specific threat intelligence. Our pilot program is evaluating additional services for release.

Hundreds of industry partners of all sizes and complexities have already signed up for NSA's cybersecurity services, which has helped protect these networks against malicious cyber activity. The no-cost cybersecurity services have also assisted with the early identification, exposure, and remediation of multiple nation-state campaigns targeting the DIB.

Scaling cybersecurity across the DIB requires continued collaboration. For more information, go to nsa.gov/ccc and 'Get Started'. A representative from the NSA CCC DIB Defense Team will reach out to provide an overview of the program and the associated benefits.

NATIONAL SECURITY AGENCY CYBERSECURITY SERVICES



Drive Down Risk, Protect DoD Information

NSA is offering companies with an active DoD contract (sub or prime), or with access to non-public, DoD information, several threat-informed cybersecurity solutions to help reduce risk of network compromise and protect sensitive but unclassified information.

Benefits



Receive NSA Threat Intel

Partner with NSA on non-public, DIB-specific NSA threat intelligence



Improve Network Defense

Our services will help increase the security of your networks



Attain Mitigation Guidance

We provide guidance to mitigate the vulnerabilities illuminated using our services



Engage Privately

All partnerships are underpinned by Non-Disclosure Agreements (NDAs)



CMMC Support

Our services support several NIST 800-171 requirements for Risk Assessment, System and Communications Protection, and System and Information Integrity families of requirements.

Success By the Numbers

- Blocked **1B** instances of known malicious or suspicious cyber activity through Protective DNS
- Identified **over a million** network vulnerabilities for remediation
- Discovered **over 8,000** vulnerable host devices
- Identified **over 202,000** vulnerable Partner IPs
- Identified **almost 70,000** vulnerable connective services

OUR SERVICES



Protective Domain Name System (PDNS)

Block users from connecting to malicious or suspicious domains, driving down risk and protecting DOD information.

1.3 B Malicious/suspicious domains blocked, including nation-state spear phishing, malware, botnets, and ransomware activity.

CMMC Support - NIST 800-171 System & Information Integrity 3.14.06



Attack Surface Management

Find and fix issues before they become compromises.

Step one: identify internet-facing assets, and determine possible vulnerabilities. Step two: company receives a tailored remediation list, prioritized by severity and likeliness of exploitation based on NSA's unique insights.

CMMC Support - NIST 800-171 Risk Assessment 3.11.02, 3.11.03



Threat Intelligence Collaboration

Partner with NSA to receive non-public, DIB specific threat intelligence and the opportunity to engage on the materials being shared.

Our services have illuminated, exposed, and remediated active nation-state exploitation attempts across hundreds of enrolled customers.

CMMC Support - NIST 800-171 System & Information Integrity 3.14.03

Enrollment is Easy:

1. Click "GET STARTED" on nsa.gov/cc
2. Confirm you meet eligibility criteria
3. Sign DIB Framework agreement

Ask us about additional pilots and services!

Industry Partner Testimonial:

“ Thank you for your support during the seamless integration of the NSA Cyber Security suite for the Defense Industrial Base... Within fifteen minutes... we were able to configure our...firewall for the various services.”

