

Threat Indicator Resources and Cybersecurity Assistance

These resources provide threat indicators to help organizations detect and block cybersecurity.

Defense Industrial Base Cybersecurity (DIB CS) Program

<https://dibnet.dod.mil/portal/intranet>
Department of Defense

DoD established the DIB CS Program to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems. This public-private cybersecurity partnership is designed to improve DIB network defenses, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness. Under the DIB CS Program, DoD and DIB participants share unclassified and classified cyber threat information.

Cyber Assistance Team (CAT)

MDAcyberassistanceteam@mda.mil
Missile Defense Agency (MDA)

The MDA CAT mission is to (1) Improve DIB Cybersecurity posture through threat-based reviews of company networks and creation of tailored mitigation strategies. (2) Strengthen and secure BMDS technical advantage by partnering with MDA DIB to protect critical BMDS data. (3) Share DoD cyber threat information, unclassified and classified, with DIB partners and other government organizations. CAT support to vendors is by request and voluntary.

Cyber Resilience Review (CRR)

<http://www.us-cert.gov/resources/assessments>
Department of Homeland Security

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.

Defense Cyber Crime Center

<https://www.dc3.mil/>
Department of Defense

DC3 is designated as a federal cyber center and Department of Defense center of excellence, and serves as the operational focal point for the Defense Industrial Base Cybersecurity Program. DC3 operates under the executive agency of the Secretary of the Air Force Defense Industrial Base Cyber Security/Information Assurance is open to defense contractors with a National Industrial Security Program Facility Security Clearance with approved safeguarding for at least Secret information and a Communication Security account with access to DOD secure transmission systems.

DC3's mission is to deliver superior digital and multimedia forensic services, cyber technical training, vulnerability sharing, technical solutions development, and cyber analysis within the following DoD mission areas: cybersecurity and critical infrastructure protection, law enforcement and counterintelligence, document and media exploitation, and counterterrorism.

Cybersecurity and Infrastructure Security Agency (CISA)

<https://www.us-cert.gov/>
Department of Homeland Security

CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build a more secure and resilient infrastructure for the future. CISA provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management and puts it into practice to protect the Nation's essential resources.

NIST Small Business Cybersecurity Corner

www.nist.gov/itl/smallbusinesscyber
National Institute of Science and Technology (NIST)

Provides cybersecurity basics, planning guides, guidance, reference on how to respond to a cyber-incident, and other cybersecurity-related training.

MDA's DEFENSE INDUSTRIAL BASE PARTNERS

CYBERSECURITY RESOURCES



MDAcybersec-acq@mda.mil

A listing of Federal Government and Federally Funded resources available to MDA's Defense Industry Base.

DoD Cybersecurity Certification Policy and Initiatives

To assess compliance.

Cybersecurity Maturity Model Certification (CMMC)

<https://www.acq.osd.mil/cmmc/index.html>
Office of the Under Secretary of Defense for Acquisition and Sustainment OUSD(A&S)

CMMC is a DoD certification process that measures a DIB sector company's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

Defense Contract Management Agency

DIBCAC Mission: Support the warfighter by assessing the Defense Industrial Base compliance in the protection of DoD Controlled Unclassified Information, ensuring contractors implement appropriate cybersecurity requirements, in support of acquisition decision making.

NIST Resources

NIST SP 800-171 Rev.1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf>
National Institute for Science and Technology (NIST)

NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf>
National Institute for Science and Technology (NIST)

NIST Handbook 162, Self-Assessment Handbook for Assessing Security Requirements in Response to DFARS Cybersecurity Requirements

<https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>
National Institute for Science and Technology (NIST)

DoD Cybersecurity Contract Requirements

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

<https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>
Department of Defense

Requires contractors and subcontractors to:

1. Provide adequate security* to safeguard covered defense information that resides on or is transiting through a contractor's internal information system or network
2. Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
4. If requested, submit media and additional information to support damage assessment
5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information

**NIST SP 800-171 Rev.1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

Public Cybersecurity Awareness and Outreach Resources

These programs educate organizations about cybersecurity.

Controlled Unclassified Information (CUI) Registry

<https://www.archives.gov/cui>
National Archives

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice.

National Cybersecurity Awareness Month

<https://www.dhs.gov/national-cyber-security-awareness-month>
Department of Homeland Security

Private and Public entities collaborate each October to raise awareness of cybersecurity issues. The program uses materials from existing cybersecurity awareness and education resources to assist the public.

Federal Virtual Training Environment (FedVTE)

<https://fedvte.usalearning.gov/>
Department of Homeland Security

FedVTE provides free online cybersecurity training to federal, state, local, tribal and territorial government employees, contractors, and veterans.

InfraGard

<https://www.infragard.org/>
Federal Bureau of Investigation (FBI)

A network of individuals from private industry, academia, the FBI, and other government agencies that share threat information, including cyber threat information.



MDAcybersec-acq@mda.mil