AN OFFERING IN THE BLUE CYBER SERIES:

HACKERS ARE WATCHING YOU!

DoD Cyber Threat Resources

Version 14 Sep 2021

#12 in the Blue Cyber Education Series
Federal Acquisition Regulation (FAR) and DFARS

Small Business contracts contain many FARS and DFARS, some are listed and some are referenced, and you have to look them up. These are not all, but some key security requirements.

What is a DFARS? The Defense Federal Acquisition Regulation Supplement (DFARS) contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public.
DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- Report cyber incidents
- Submit malicious software
- Facilitate damage assessment
- Safeguard covered defense information
Cyber Incident Reporting and Resources

Welcome to the DIBNet portal
DoD’s gateway for defense contractor reporting and voluntary participation in DoD’s DIB Cybersecurity Program.

Cyber Reports

- Report a Cyber Incident

A DoD-approved Medium Assurance Certificate is required to report a Cyber Incident. Applying to the DIB CS Program is not a prerequisite to report.

- DoDAR 252-3-2012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- DoDAR 252-239-2018 Cloud Computing Services
- FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Bhopal Unit and Other Covered Entities
- FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?
- Contact DoD Cyber Crime Center (DC3)
- (DoD) 517-2174
- Toll Free: (877) 338-2174

DoD’s DIB Cybersecurity (CS) Program

- Apply Now!

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

- DIB CS Participant Login
- Voluntary Report

Cyber Threat Roundup
The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. For the latest edition of the Cyber Threat Roundup, please click here.

For more information about other products, please apply to the DIB CS Program.

Need Assistance?
- Contact the DIB CS Program Office
- DOD.DIB-CSM@naval-mil
- Hotline: (703) 604-3167
- Toll Free: (855) DOD-IACS
- Fax: (703) 372-5434

A DoD-approved Medium Assurance Certificate is required to access DIBNet services. To obtain a DoD-approved Medium Assurance Certificate, please click here.
Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

Hackers Leak Passwords for 500,000 Fortinet VPN Accounts ................................................................. 2
Zoho Patches Actively Exploited Critical AD Self-Service Plus Bug .......................................................... 2
GitHub Finds 7 Code Execution Vulnerabilities in `tar` and npm CLI .......................................................... 2
LockBit 2.0: Ransomware Attacks Surge after Successful Affiliate Recruitment ....................................... 2
Microsoft Fixes Bug Letting Hackers Take Over Azure Containers .............................................................. 3
DOD-DEFENSE INDUSTRIAL BASE (DIB) COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE)

The DoD Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) serves as the single DoD focal point for receiving all cyber incident reporting affecting unclassified networks of DOD contractors to safeguard DoD information.

DCISE Overview

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE)—DCISE is the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program, focused on protecting intellectual property and safeguarding DoD content residing on or transmitting through, contractor unclassified networks. The public-private cybersecurity partnership provides a collaborative environment from crowd-sourced threat sharing at both unclassified and classified levels. CDC cyber resilience analysis, and Cybersecurity-as-a-service pilot offerings. DCISE performs cyber analysis and diagnostics, offers mitigation and remediation strategies, provides best practices, and conduct analyst-to-analyst exchanges with DIB participants ranging in size from small to enterprise-sized companies.

DC3 DCISE is the reporting and analysis hub for implementation of Section 941 of the Fiscal Year 2013 National Defense Authorization Act regarding certain types of cyber incidents by Closed Defense Contractors (CDCs) and the related Defense Federal Acquisition Regulation Supplement (DFARs) 262.204-7012). Cyber incidents reported in the DFARS are submitted to DC3/DCISE as mandatory reports. However, all other cyber events can be reported voluntarily.

- Rated as Capability Maturity Model Integration for Services (CMMI-SV) Maturity Level 3
- Collaborative partnership with over 65,000 CDCs and U.S. Government (USG) agencies
- Shared over 450,000 actionable, non-attributable (to submitting source) indicators
- Provided over 77,000 hours of no-cost forensics and malware analysis for DIB Partners
- Distributed 12,500 cyber threat reports for both DIB and USG consumption (DIB partners may access DCISE reporting via their DISNET accounts and USG members can access via SIBS Interhake)
- Operates 24/7/365 DCISE support hotline to assist subcontractors and DIB & USG Partners

Contact Us

Phone: 410-981-0104
Toll Free: 1-877-935-2174
Email: DCISE@dc3.mil

Click to subscribe and receive future communications and updates.

DIBNET PORTAL

DIB's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.
DoD CYBER CRIME CENTER

Contact Us:
Executive Support Staff
410-981-1181
ExecutiveSupport@dc3.mil

Cyber Forensics Laboratory (CFL)
CFL@dc3.mil
National Center for Digital Forensics
Academic Excellence:
CDFAE@dc3.mil

Cyber Training Academy (CTA)
Registrar: CTARegistrar@dcia.edu

DoD-DIB Collaborative Information
Sharing Environment (DOISE)
DOISE@dc3.mil

Operations Enablement Directorate (OED)
OED.Info@dc3.mil

Technical Solutions Development (TSD)
TSD@dc3.mil

Vulnerability Disclosure Program (VDP)
VDP. Questions@dc3.mil

Public Affairs
410-981-6610
INFO@dc3.mil

DC3 CAPABILITIES FOR DoD REQUIREMENTS

FORENSIC LAB SERVICES
DoD Center of Excellence for Digital and Multimedia (D/MM) forensics, DC3 Cyber Forensics Lab is an ISO 17025 accredited lab that performs D/MM forensic examinations, device repair, data extraction, and expert testimony for DoD.
- Network Intrusions
- Malware/Reverse Engineering
- Enhancing Video and Voice Recordings
- Aircraft Mishap Data Recovery
- Damaged Media and Submerged Devices
- Mobile Device Encryption/Recovery
- DOMEX Forensic Partner

DEFENSE INDUSTRY SHARING
DoD focal point for all cyber incident reporting affecting unclassified networks of Defense Industrial Base (DIB) contractors.
- Cyber Threat Information Sharing with DIB
- Cyber Incident and Malware Analysis
- Pilot Service Offerings (CSaaS)
- Mitigation and Remediation Strategies
- Partnership Exchanges
- Cyber Resiliency Analyses

MISSION STATEMENT
Deliver superior digital and multimedia (D/MM) 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.

VISION STATEMENT
Digital and multimedia technical and analytical center of excellence to improve DoD mission assurance and enhance warfighter capability.

OPERATIONS ENABLEMENT
Amplifies the collective effects of DoD-wide law enforcement and counterintelligence investigations and operations by conducting expert technical analysis and all-source analysis and developing enhanced operational support capabilities.
- Collaborative Analytics with LE/CJIC
- Focused All Source Intelligence
- Tailored Operational Production
- StormSystem Enhancement and Deployment
- CADO-IS Development and Integration

CYBER TRAINING
Provides specialized in-residence and online cyber training (www.dcita.edu).
- Cyber Protection Team Training
- Network Defense
- Computer Technologies
- Basic and Advanced Forensic Examination
- Distance Learning/Webinar/Mobile Training
- Digital Forensics Certifications

VULNERABILITY MANAGEMENT
DoD Vulnerability Disclosure Program Lead. Includes collaborative efforts with private-sector cybersecurity researchers to crowdsource the identification of vulnerabilities on DoD networks and systems.
- Enhance Security of DoD Networks/Systems
- Independent Assessment of Cyber Defenses
- Improve Mission Assurance

TECHNICAL SOLUTIONS
Tailored software and system solutions to support digital forensic examiners, DOMEX, and cyber intrusion analysis.
- Tool and Software Development
- Tool Test/Validation (Including GOTS/COTS)
- Counterintelligence Tool Repository
- Automated Malware Processing

CISA – Cybersecurity & Infrastructure Security Agency

Resources for Small and Midsize Businesses (SMB)

Cyber Essentials
CISA’s Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

Cybersecurity Resources Road Map (A Guide for Critical Infrastructure SMBs)
The Cybersecurity Resources Road Map is a guide for identifying useful cybersecurity best practices and resources based on needs.

Stop, Think, Connect. Toolkit
The Stop, Think, Connect.™ campaign includes cybersecurity tips for SMBs.
Five products in the National Cyber Awareness System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips.

A subscription to any or all of the National Cyber Awareness System products ensures that you have access to timely information about security topics and threats. To learn more or to subscribe, visit the subscription system. You can also visit our Mailing Lists and Feeds page to learn more about how to subscribe or use our syndicated feeds. If you're having trouble subscribing, read the FAQ.

- Check out our tips and security publications for additional security information.
TIPS & TACTICS | PREPARING YOUR ORGANIZATION FOR RANSOMWARE ATTACKS

HOW DO I STAY PREPARED?

What do you do if your computer suddenly displays a countdown clock and a message telling you that your files have been encrypted and will be permanently lost to you unless you pay a ransom by a specified date and time? Whether you are responsible for protecting computers and data for a small business, hospital, local government, or other organization, it’s vital that you be prepared for ransomware attacks. This guidance from the National Institute of Standards and Technology (NIST) includes basic practices for protecting against and recovering from ransomware attacks. Be sure to consult an expert if one is available to you.

PROTECTING AGAINST THE THREAT

The computers and information on which we rely are under constant threat from disruptive and potentially destructive ransomware. NIST recommends that organizations take these basic steps to help thwart ransomware:

- Avoid using personal applications and websites, such as email, chat, and social media, from work computers.
- Avoid opening files, clicking on links, etc. from unknown sources without first checking them for suspicious content. For example, you can run an antivirus scan on a file, or look at a link to see if it goes to the site it claims to be going to.
- NIST’s National Cybersecurity Center of Excellence (NCCoE) has collaborated with the private sector on projects that can help organizations protect themselves against future ransomware attacks. An example is Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (NIST Special Publication 1800-28).
- Users should follow these tips for their work computers:
  - Use antivirus software at all times—and make sure it’s set up to automatically scan your emails and removable media (e.g., flash drives) for ransomware and other malware.
  - Keep all computers fully patched.
  - Use security products or services that block access to known ransomware sites on the internet.
  - Configure operating systems or use third-party software to allow only authorized applications to run on computers, thus preventing ransomware from working.
  - Restrict or prohibit use of personally owned devices on the organization’s networks and for telework/remote access without taking extra steps to assure security.

Users should follow these tips for their work computers:

Quick steps you can take now to PROTECT yourself from the threat of ransomware:

1. USE ANTI-VIRUS SOFTWARE AT ALL TIMES
   - Set your software to automatically scan emails and flash drives.

2. KEEP YOUR COMPUTER FULLY PATCHED
   - Run scheduled checks to keep everything up-to-date.

3. BLOCK ACCESS TO RANSOMWARE SITES
   - Use security products or services that block access to known ransomware sites.

4. ALLOW ONLY AUTHORIZED APPS
   - Configure operating systems or use third-party software to allow only authorized applications on computers.

5. RESTRICT PERSONALLY-OWNED DEVICES
   - Organizations should restrict or prohibit access to official networks from personally-owned devices.

6. USE STANDARD USER ACCOUNTS
   - Organizations should restrict or prohibit access to official networks from personally-owned devices.


Organizations without dedicated cybersecurity professionals should consider establishing relationships with third-party cybersecurity service providers and using their expertise to assist in
Center for Internet Security - CIS

CIS Controls
Follow our prioritized set of actions to protect your organization and data from known cyber-attack vectors.

Download CIS Controls v8

Learn about Implementation Groups
View All 18 CIS Controls
Join a Community

CIS Controls v7.1 is still available. Learn more about CIS Controls v7.1
NIST Small Business Cybersecurity
Cybersecurity Risks

This page includes resources that provide overviews of cybersecurity risk and threats and how to manage those threats. The Risks & Threats section includes resources that includes threats and risks like ransomware, spyware, phishing and website security. The Risk Management section includes resources that describe the importance of managing risk and common security risk and mitigations misunderstandings.

RISKS & THREATS

Protecting Against Malicious Code – a description of viruses, worms, and Trojan horses and tips for protecting your business from these types of malicious code
Department of Homeland Security

Handling Destructive Malware – an overview of the threat of destructive malware, potential distribution vectors, and tips for protecting your business
Department of Homeland Security

Understanding Hidden Threats: Rootkits and Botnets – an overview of rootkits and botnets and tips for protecting your business
Department of Homeland Security

Recognizing Fake Antivirus – description of the fake antivirus threat and tips for avoiding and recovering from fake antivirus software
Department of Homeland Security

Understanding Hidden Threats: Corrupted Software Files – an overview of how malicious files can impact your electronic devices and tips for protecting your business
Department of Homeland Security
The National Institute of Standards and Technology (NIST) defines a vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [Source] NIST defines a risk as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence. [Source]
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event Description</th>
<th>Location</th>
<th>Cost</th>
<th>Register</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, September 21</td>
<td>8:30-10:30 am HST</td>
<td>&quot;CMMC - A Primer&quot; Cybersecurity Maturity Model Certification Framework and Compliance, Levels 1-3</td>
<td>Online event</td>
<td>$0.00</td>
<td>REGISTER</td>
</tr>
<tr>
<td>Thursday, September 23</td>
<td>9-10:30 am EDT</td>
<td>SBA Business Development Program</td>
<td>Online event</td>
<td>$0.00</td>
<td>REGISTER</td>
</tr>
<tr>
<td>Tuesday, October 5</td>
<td>9-10 am CDT</td>
<td>Cybersecurity Maturity Model Certification (CMMC): Webinar - A Legal Overview</td>
<td>Online event</td>
<td>$0.00</td>
<td>REGISTER</td>
</tr>
<tr>
<td>Tuesday, October 5</td>
<td>9-10 am CDT</td>
<td>Cybersecurity Maturity Model Certification (CMMC): A Legal Overview</td>
<td>Online event</td>
<td>$0.00</td>
<td>REGISTER</td>
</tr>
<tr>
<td>Tuesday, October 5</td>
<td>11 am-12 pm MDT</td>
<td>Protecting Your Business from Cybercrime: 2021-22 Cybersecurity Updates</td>
<td>Online event</td>
<td>$0.00</td>
<td>REGISTER</td>
</tr>
</tbody>
</table>
StopThinkConnect.org Cybersecurity Training

PARTNER WITH US
Incorporate STOP. THINK. CONNECT. into your online safety efforts

Learn More
www.staysafeonline.org/events
www.staysafeonline.org/events

Upcoming Events

General

Cyber Talent CIO Forum

Virtual | 12:30 pm - 4:30 pm (EST)

Join technology, business and cybersecurity leaders who are rising to the National Cyber Scholarship Foundation's 25x25 Challenge to discover and train a diverse new generation of 25,000 cyber stars by the year 2025! This free virtual event will be held on July 21, 2021 12:30 pm EST!

EVENT DETAILS  RSVP 

Cybersecurity Awareness Month | National Cyber Security Alliance

How to Get Involved in Cybersecurity Awareness Month 2021
References

- DIBNET: www.dibnet.dod.mil
- CISA: www.CISA.gov/cybersecurity
- STOPRANSOMEWARE.GOV
- NIST: www.csrc.nist.gov or www.nist.gov/smallbusinesscyber
- Center for Internet Security: www.cisecurity.org/controls
- DIB CyberAssist: www.ndisac.org
- FBI: www.ic3.gov
- SBA Events: www.sba.gov/events
Any Questions?

- This briefing is not a substitute for reading the FARs and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: [www.safcn.af.mil/ciso/](http://www.safcn.af.mil/ciso/)
  - Select Quick Link: Small Business Cybersecurity Information
- Please provide questions, feedback or if you just want to talk about your cybersecurity/data protection questions to Kelley.Kiernan@us.af.mil
  - Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!
DAF CISO webpage

www.safcn.af.mil/ciso/

Select Quick Link: Small Business Cybersecurity Information