

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 contains many FARs and DFARS, some are listed 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
252.239-7010
Cloud Computing
Services

FAR Clause
252.204-21
Basic Safeguarding
of Covered
Contractor
Information Systems

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

DFARS Clause
252.204-7008
Compliance with
safeguarding
covered defense
information controls

DFARS Clause
252.204-7019
NIST SP 800-171
DoD Assessment
Requirements.

DFARS Clause
252.204-7021
Cybersecurity
Maturity Model
Certification
Requirement



AFWERX
SBIR★STTR

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





AFWERX
SBIR★STTR

<https://dibnet.dod.mil/portal/intranet/>

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 [Medium Assurance Certificate](#) is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

[DFARS 252.204-7012](#) Safeguarding Covered Defense Information and Cyber Incident Reporting

[DFARS 252.239-7010](#) Cloud Computing Services

[FAR 52.204-23](#) Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab 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)

DCISE@dc3.mil

Hotline: (410) 981-0104

Toll Free: (877) 838-2174

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

OSD.DIBCSIA@mail.mil

Hotline: (703) 604-3167

Toll Free: (855) DoD-IACS

Fax: (571) 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](#).



AFWERX
SBIR★STTR



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

10 September 2021

Cyber Threat Roundup

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


Contents

Articles.....	2
Hackers Leak Passwords for 500,000 Fortinet VPN Accounts.....	2
Zoho Patches Actively Exploited Critical ADSelfService 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



AFWERX
SBIR★STTR

<https://www.dc3.mil/Organizations/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/>



DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)
A FEDERAL CYBER CENTER

Search DC3

ABOUT DC3 ▾DC3 LEADERSHIP ▾NEWS ▾EMPLOYMENT ▾ORGANIZATIONS ▾PRODUCTS ▾RESOURCES ▾TOOLS ▾CONTACT US ▾

ABOUT DC3 > ORGANIZATIONS > DIB CYBERSECURITY > DIB CYBERSECURITY (DCISE)

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 transiting 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 Cleared Defense Contractors (CDCs), and the related Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012). Cyber incidents outlined 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-SVC) Maturity Level 3
- Collaborative partnership with over 85,000 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
- Disseminated 12,500+ cyber threat reports for both DIB and USG consumption (DIB partners may access DCISE reporting via their DIBNET accounts and USG members can access via SIPR Intelshare)
- Operates 24/7/365 DCISE support hotline to assist submitters and DIB & USG Partners

DCISE Fact Sheet


DCISE Slick Sheets

DCISE News

Contact Us ▶

Phone: 410-981-0104
Toll Free: 1-877-838-2174

Email: DCISE@dc3.mil

 DCISE

Click to subscribe and receive future communications and updates.

DIBNET PORTAL

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

DIB Cyber Reports


DIB CS Program

DIB



AFWERX
SBIR★STTR

<https://www.dc3.mil/Organizations/DIB-Cybersecurity/DCISE-Slick-Sheets/>



DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)
A FEDERAL CYBER CENTER

Search DC3

ABOUT DC3 ▾DC3 LEADERSHIP ▾NEWS ▾EMPLOYMENT ▾ORGANIZATIONS ▾PRODUCTS ▾RESOURCES ▾TOOLS ▾CONTACT US ▾

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.

ABOUT DC3 > ORGANIZATIONS > DIB CYBERSECURITY > DCISE SLICK SHEETS

DCISE Slick Sheets

DCISE Recommended Top 5

[DCISE Recommended Top 5 Cyber Security Best Practices For Small and Medium Companies](#)

The Threat is Real

[The Threat is Real](#)

Analytics

DIB-Reported Cyber Threats

[CY2021 Q1: January - March](#)

[CY2021 Q2: April - June](#)

Maritime Industry

[Cyber Threats to Maritime Industry](#)

Transportation Industry

[Cyber Threats to Transportation Industry](#)

Aerospace Industry

[Cyber Threats to Aerospace Industry](#)

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: CTA.Registrar@dcita.edu

**DoD-DIB Collaborative Information
Sharing Environment (DCISE)**
DCISE@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

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

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/CI/IC
- 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

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







AFWERX
SBIR ★ STTR

www.CISA.gov/cybersecurity

CISA – Cybersecurity & Infrastructure Security Agency

An official website of the United States government [Here's how you know](#) [EMAIL US](#) [CONTACT](#) [SITE MAP](#)

 **CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY** 

[CYBERSECURITY](#) [INFRASTRUCTURE SECURITY](#) [EMERGENCY COMMUNICATIONS](#) [NATIONAL RISK MANAGEMENT](#) [ABOUT CISA](#) [MEDIA](#)

CYBERSECURITY

CISA leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life.

Quick Links

CISA Insights	Supply Chain Compromise	Ransomware Guidance and Resources
Combating Cyber Crime	Cybersecurity Governance	Cyber Hygiene Services
Coordinated Vulnerability Disclosure	Cybersecurity Insurance	Information Sharing
Cyber Essentials	Cybersecurity Training & Exercises	Protecting Critical Infrastructure
Cyber Incident Response	Detection and Prevention	Securing Federal Networks
Cyber Safety	Education	Shop Safely
Cyber Resource Hub	EO 13800 Deliverables	

Nation State Cyber Threats

 China	 Russia	 North Korea	 Iran
--	---	--	---

 DIRECTIVES & GUIDANCE	 INFORMATION SHARING	 PROTECTING CRITICAL INFRASTRUCTURE	 SECURING FEDERAL NETWORKS	 TIPS & ALERTS
--	--	---	--	--




AFWERX
SBIR★STTR


www.CISA.gov/resources/smb

CISA – Cybersecurity & Infrastructure Security Agency

An official website of the United States government Here's how you know



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



Services

Report

Alerts and Tips Resources Industrial Control Systems

Resources > Resources for Small and Midsize Businesses (SMB)

Cybersecurity Framework

Academia

Business

Federal Government

Small and Midsize Businesses

SLTT Government

Assessments

Events and Media

Related Resources

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.

Note to cybersecurity trainers and small business advisors:

To professionally print the Cybersecurity Resources Road Map at a print shop (trifold brochure) for distribution to businesses at training events and workshops, use this [print shop version of the Road Map](#) and these [printing instructions](#).

Stop.Think.Connect. Toolkit

The [Stop.Think.Connect.™](#) campaign includes cybersecurity tips for SMBs.



[Alerts and Tips](#) ▾[Resources](#)[Industrial Control Systems](#)

National Cyber Awareness System

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.

Current Activity

Provides up-to-date information about high-impact types of security activity affecting the community at large.

[View Current Activity](#) >

Alerts

Provide timely information about current security issues, vulnerabilities, and exploits.

[View Alerts](#) >

Bulletins

Provide weekly summaries of new vulnerabilities. Patch information is provided when available.

[View Bulletins](#) >

Analysis Reports


Provide in-depth analysis on a new or evolving cyber threat.

[View Analysis Reports](#) >




AFWERX
SBIR★STTR

StopRansomware.gov

 An official website of the United States government [Here's how you know](#) ▼

STOP RANSOMWARE

Search 

RESOURCES NEWSROOM ALERTS REPORT RANSOMWARE

WHAT IS RANSOMWARE?

[LEARN MORE](#)

HAVE YOU BEEN HIT BY RANSOMWARE?

[LEARN MORE](#)

AVOID BEING HIT BY RANSOMWARE

[LEARN MORE](#)



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:**

- **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:

- **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 [SP] 1800-25).

Learn more about NIST NCCoE projects to improve data security practices at: <https://nccoe.nist.gov/projects/building-blocks/data-security>.

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

TIPS & TACTICS RANSOMWARE



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

- 1 USE ANTIVIRUS 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**





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](#)

CIS Controls v8 Resources and Tools

[Learn about Implementation Groups](#)

[View All 18 CIS Controls](#)

CIS Controls Community
[Join a Community](#)

CIS Controls v7.1 is still available
[Learn more about CIS Controls v7.1](#)



AFWERX
SBIR ★ STTR

www.nist.gov/smallbusinesscyber

NIST Small Business Cybersecurity

NIST

Search NIST

Menu

Information Technology Laboratory

SMALL BUSINESS CYBERSECURITY CORNER

Cybersecurity Basics +

Planning Guides +

Guidance by Topic +

Responding to a Cyber Incident

Training

Partners

About & Contact Us

CONNECT WITH US

Your resource for keeping your small business secure.

Get cybersecurity basics, guidance, solutions, and training to protect your information and manage your cybersecurity risks.

SPOTLIGHT

Data Compromised?

Planning Guides

Cybersecurity Basics



Cybersecurity Basics

Cybersecurity Risks

For Managers

Case Study Series

Glossary

Planning Guides

Guidance by Topic

Responding to a Cyber Incident

Training

Partners

About & Contact Us

CONNECT WITH US



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 Antiviruses](#) – 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




DIB CyberAssist www.ndisac.org




AWARENESSIMPLEMENTATION & ASSESSMENTCMMCABOUT CYBERASSISTSEARCH

Home > Implementation And Assessment > Vulnerability And Risk Management


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. [\(Source\)](#)




Anti-Malware



Penetration Testing



System Patching &
Vulnerability Remediation



Vulnerability Scanning

CONTACT INFORESOURCESLEGALSTAY CONNECTED. REGISTER TO RECEIVE
REGULAR UPDATES



AFWERX
SBIR★STTR

www.ic3.gov

FBI Internet Crime Complaint Center - IC3



FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center IC3





AFWERX
SBIR ★ STTR

www.sba.gov/events



Small Business Administration

Tuesday, September 21 8:30–10:30 am HST	“CMMC –A Primer” Cybersecurity Maturity Model Certification Framework and Compliance, Levels1-3 Online event	\$0.00	REGISTER
Thursday, September 23 9–10:30 am EDT	8(a) Business Development Program Online event	\$0.00	REGISTER
Tuesday, October 5 9–10 am CDT	Cybersecurity Maturity Model Certification (CMMC) Webinar– A Legal Overview Online event	\$0.00	REGISTER
Tuesday, October 5 9–10 am CDT	Cybersecurity Maturity Model Certification (CMMC), A Legal Overview Online event	\$0.00	REGISTER
Tuesday, October 5 11 am–12 pm MDT	Protecting Your Business from Cybercrime- 2021-22 Cybersecurity Updates Online event	\$0.00	REGISTER

13



AFWERX
SBIR ★ STTR

StopThinkConnect.org Cybersecurity Training





AFWERX
SBIR★STTR

www.sba.gov/local-assistance/find

Small Business Administration



[Translate](#) [SBA en Español](#) [For Partners](#) [Newsroom](#) [Contact Us](#)

[Business Guide](#) [Funding Programs](#) [Federal Contracting](#) [Learning Platform](#) [Local Assistance](#) [About SBA](#)

Find local assistance Info ▾

Business Zip Code

Provided By

Enter a 5-digit zip code.

All ▾

All

SEARCH

- SCORE Business Mentoring
- Small Business Development Center
- U.S. Export Assistance Center
- Veteran's Business Outreach Center
- Women's Business Center
- Procurement Technical Assistance Center
- Certified Development Company





AFWERX
SBIR★STTR

www.staysafeonline.org/events

NATIONAL CYBERSECURITY ALLIANCE

Stay Safe Online Our Programs Resources Library Get Involved Contact Us

ABOUT US NEWSLETTER SIGN-UP

Educating and empowering our global digital society

Our Programs

CYBERSECURITY AWARENESS MONTH

DATA PRIVACY DAY

CyberSecure MY BUSINESS



AFWERX
SBIR ★ STTR

www.staysafeonline.org/events

NATIONAL
CYBERSECURITY
ALLIANCE

ABOUT US NEWSLETTER SIGN-UP

Stay Safe Online Our Programs Resources Library Get Involved Contact Us

UPCOMING EVENTS CYBERSECURE MY BUSINESS™ DATA PRIVACY DAY CYBERSECURITY AWARENESS MONTH NATIONAL CYBER SECURITY ALLIANCE SUBMIT AN EVENT

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
- DCISE: <https://www.dc3.mil/Organizations/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/>
- DOD Cyber Crime Center: https://www.dc3.mil/Portals/100/Documents/DC3/Resources/Trifolds/DC3-Trifold-Final_26Apr21.pdf?ver=rt-N9XYyQMNV4IagCc-4rQ%3d%3d
- CISA: www.CISA.gov/cybersecurity
- STOPRANSOMWARE.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



AFWERX
SBIR ★ STTR

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/Small-Business-Cybersecurity-Information/
 - Select Quick Link: Small Business Cybersecurity Information
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to www.safcn.af.mil/Contact-Us/





AFWERX
SBIR★STTR

DAF CISO webpage

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

The screenshot shows the SAF/CN Office of the Chief Information Officer website. The header includes the SAF/CN logo and navigation links: HOME, CONTACT US, LEADERSHIP, ORGANIZATIONS, and CAREERS. The main content area is titled "SMALL BUSINESS CYBERSECURITY INFORMATION" and includes a section for "SMALL BUSINESS" with a description of SBIR and STTR programs. Below this is a section for "SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS" featuring a grid of presentation thumbnails with titles such as "Following the Cyber DFARS", "DoD Cybersecurity Incident Reporting", "Get Your SPRS On!", "Can I give my contractor CUI?", "Fast Track ATO", "Protection of Common Types of DOD CUI", "DAF Small Business Cybersecurity Resources", and "Unclassified Threat Briefing for DAF Small Businesses".