## 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

```
Mirror_mod.mirror_object
  eration == "MIRROR_X":
mirror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
  operation == "MIRROR Y"
 lrror_mod.use_x = False
 irror_mod.use_y = True
 lrror_mod.use_z = False
  operation == "MIRROR_Z"
  rror_mod.use_x = False
  rror_mod.use_y = False
  rror_mod.use_z = True
  melection at the end -add
   ob.select= 1
  er ob.select=1
   ntext.scene.objects.action
  "Selected" + str(modified
   rror ob.select = 0
  bpy.context.selected_obj
  ata.objects[one.name].sel
  int("please select exaction
     OPERATOR CLASSES -
```

TITTOT\_mod = modifier\_ob

mirror to the selected

es.Operator):

|ect.mirror\_mirror\_x\*





# 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







## 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**











10 September 2021

### **Cyber Threat Roundup**

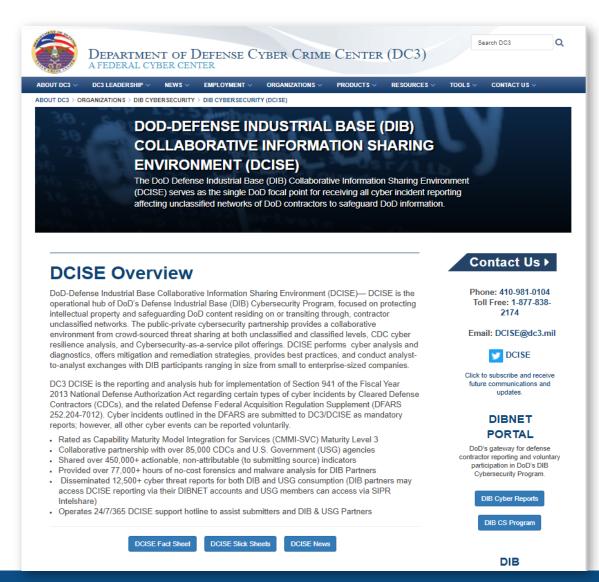
A collection of recent open-source items of interest to the Defense Industrial Base

#### 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

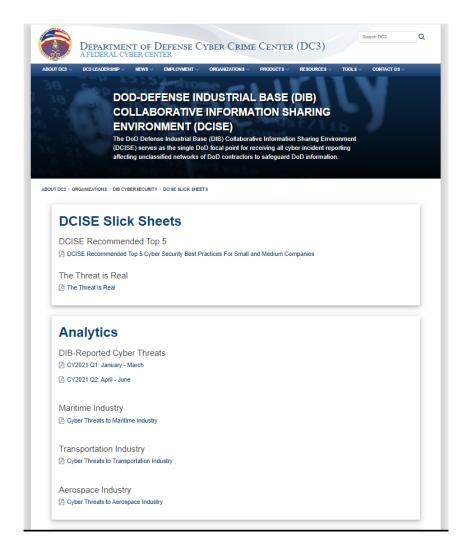














# DOD CYBER CRIME CENTER

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.

# Cyber Training Forensic Lab Services Vulnerability Disclosure DIB Cyber Threat Sharing Enablement

#### **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.

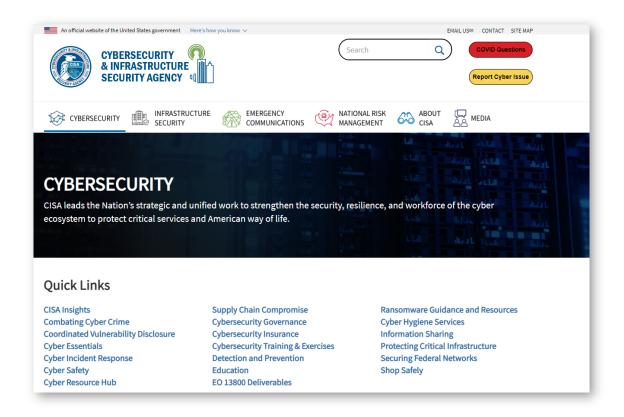
- · Tool and Software Development
- Tool Test/Validation (Including GOTS/COTS)
- Counterintelligence Tool Repository
- Automated Malware Processing

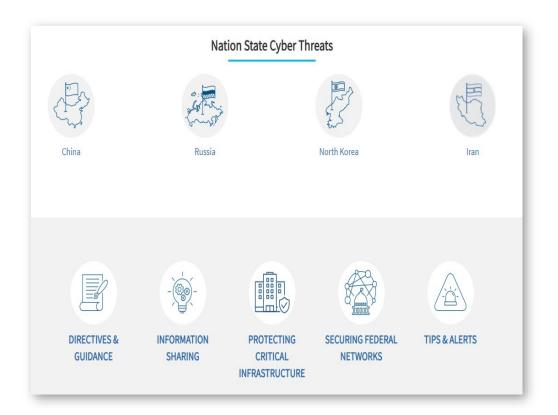






# **CISA – Cybersecurity & Infrastructure Security Agency**



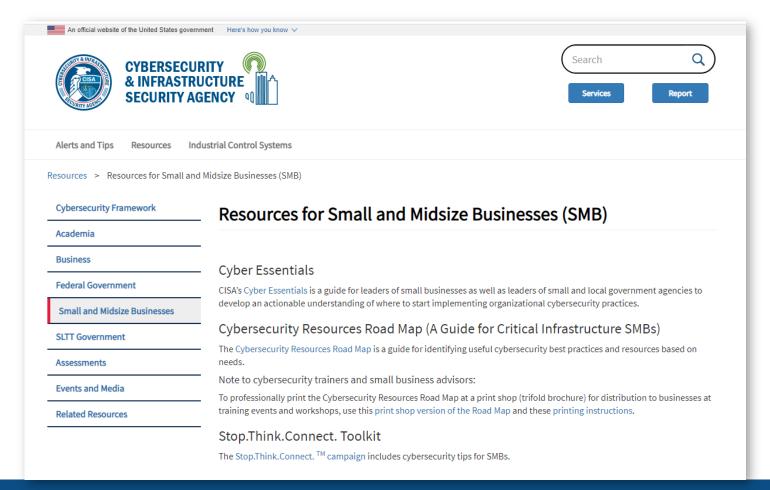






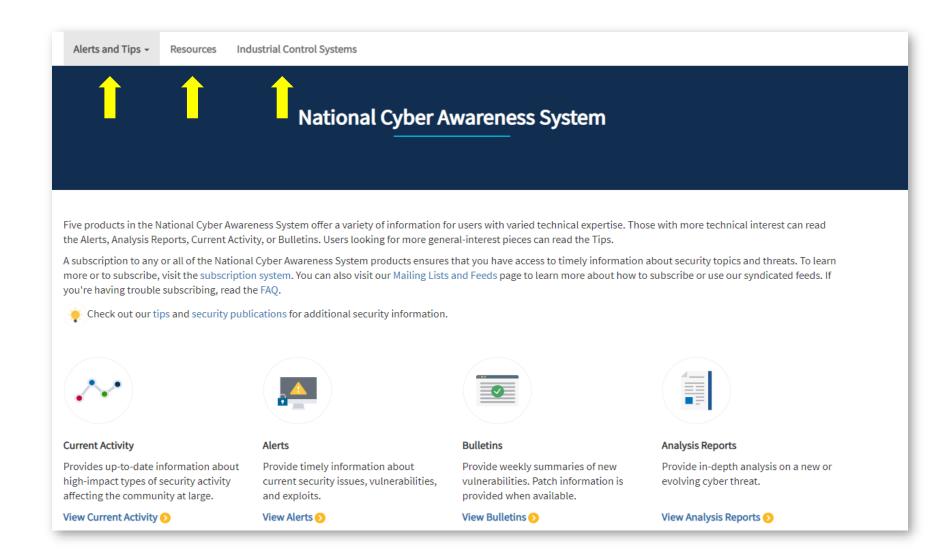


## **CISA – Cybersecurity & Infrastructure Security Agency**







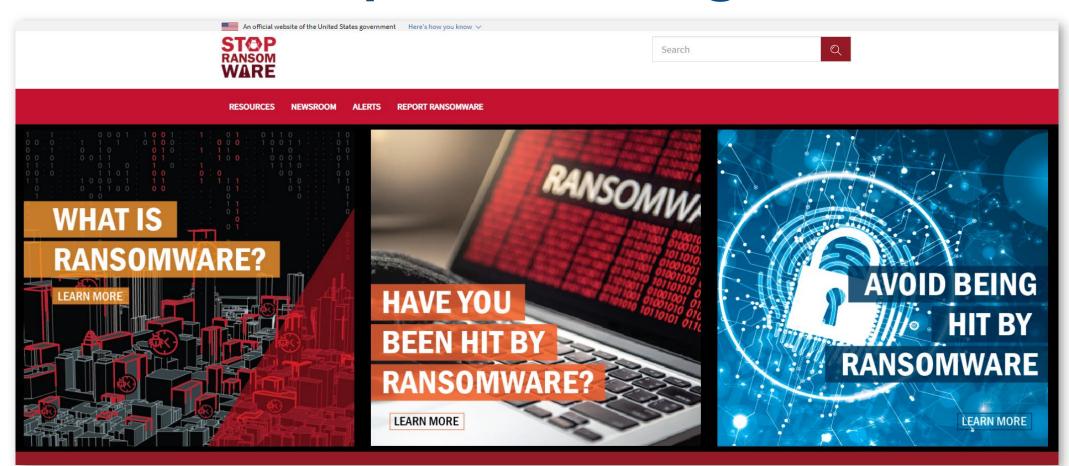








# StopRansomware.gov











## 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 <u>Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events</u> (NIST Special Publication [SP] 1800-25).

Learn more about NIST NCCoE projects to improve data security practices at:

https://nccoe.nist.gov/projects/buildingblocks/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

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.



Organizations should restrict or prohibit access to official networks from personally-owned devices.

6 USE STANDARD USER ACCOUNTS



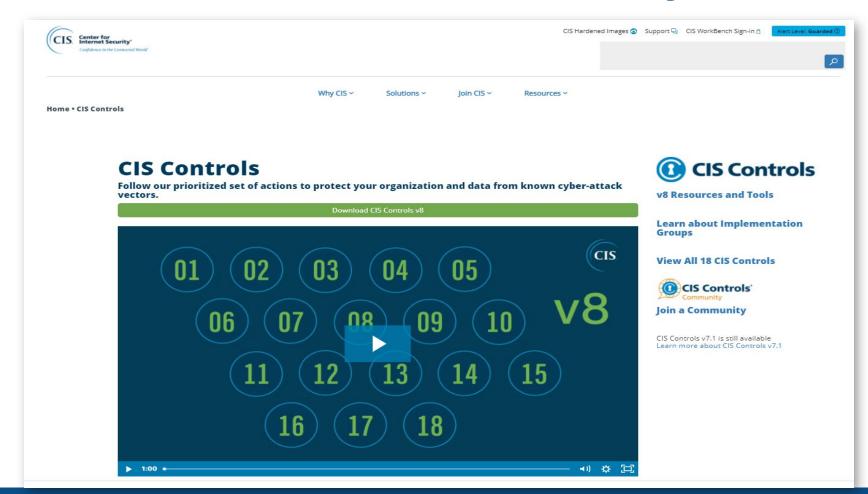








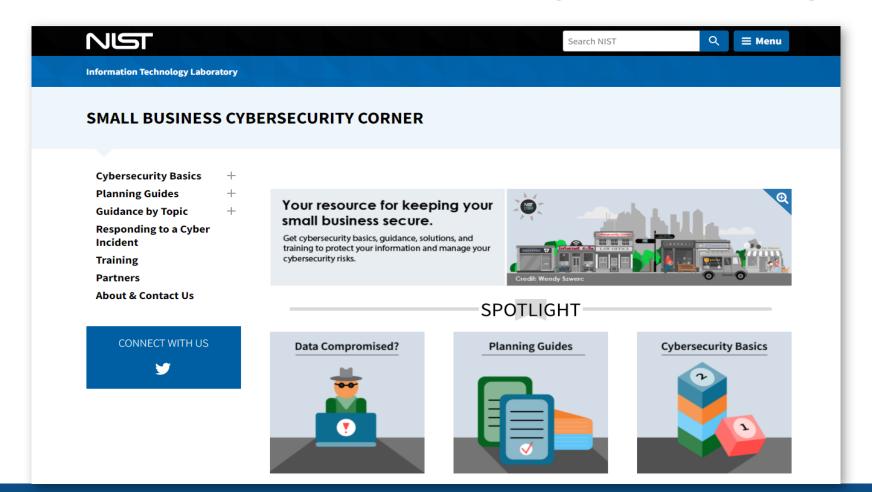
# **Center for Internet Security - CIS**







# **NIST Small Business Cybersecurity**





## 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**

<u>Protecting Against Malicious Code</u> – a description of viruses, worms, and Trojan horses and tips for protecting your business from these types of malicious code

Department of Homeland Security

<u>Handling Destructive Malware</u> – an overview of the threat of destructive malware, potential distribution vectors, and tips for protecting your business

Department of Homeland Security

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

<u>Recognizing Fake Antiviruses</u> – description of the fake antivirus threat and tips for avoiding and recovering from fake antivirus software

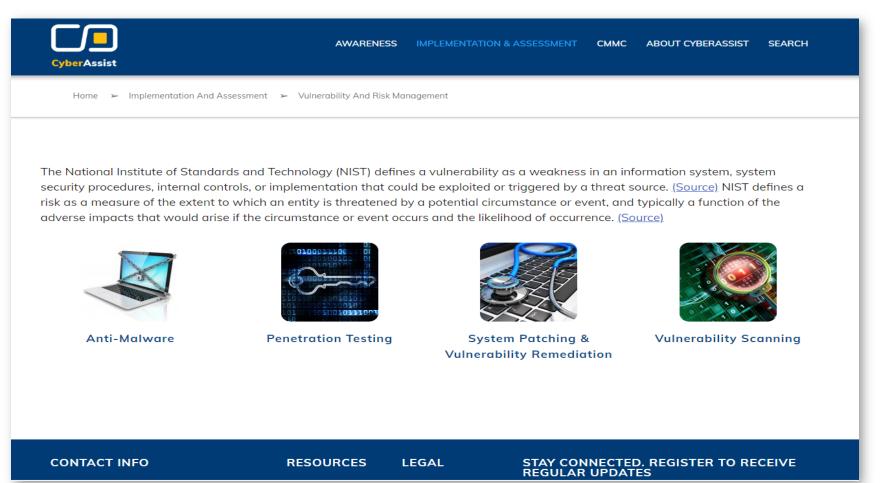
Department of Homeland Security

<u>Understanding Hidden Threats: Corrupted Software Files</u> – an overview of how malicious files can impact your electronic devices and tips for protecting your business





# DIB CyberAssist www.ndisac.org







# FBI Internet Crime Complaint Center - IC3











## **Small Business Administration**



Tuesday, September 21 8:30–10:30 am HST	<u>"CMMC – A Primer" Cybersecurity Maturity Model Certification Framework and Compliance, Levels1-3</u> Online event	\$0.00	REGISTER ☑
Thursday, September 23 9–10:30 am EDT	8(a) <u>Business Development Program</u> Online event	\$0.00	REGISTER ☑
Tuesday, October 5 9–10 am CDT	<u>Cybersecurity Maturity Model Certification (CMMC)Webinar – A Legal Overview</u> 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 ☑







# StopThinkConnect.org Cybersecurity Training

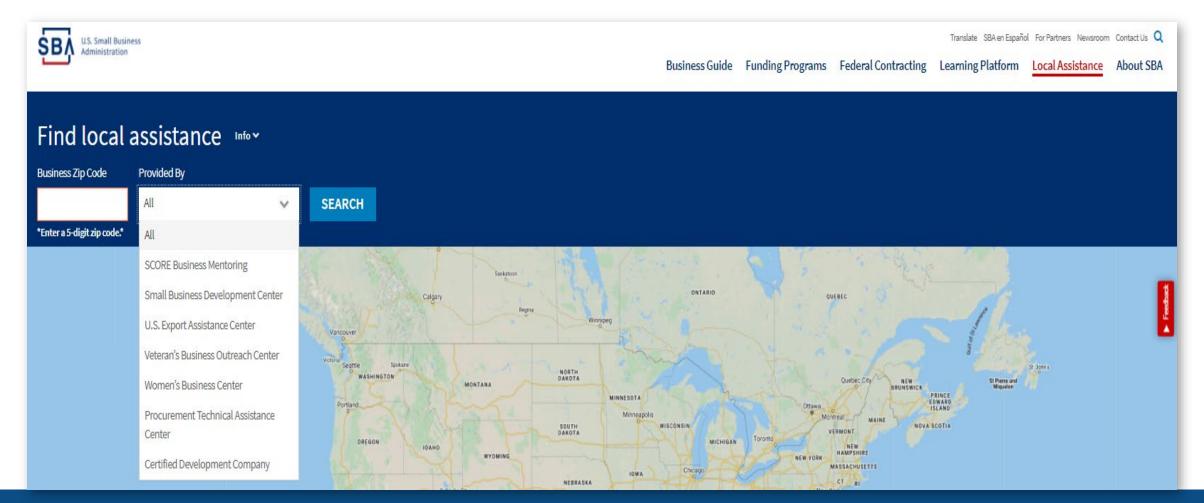








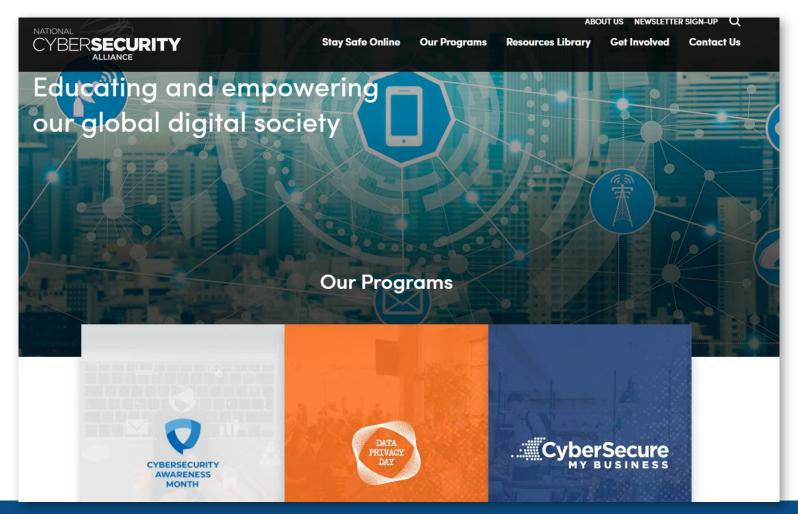
## **Small Business Administration**







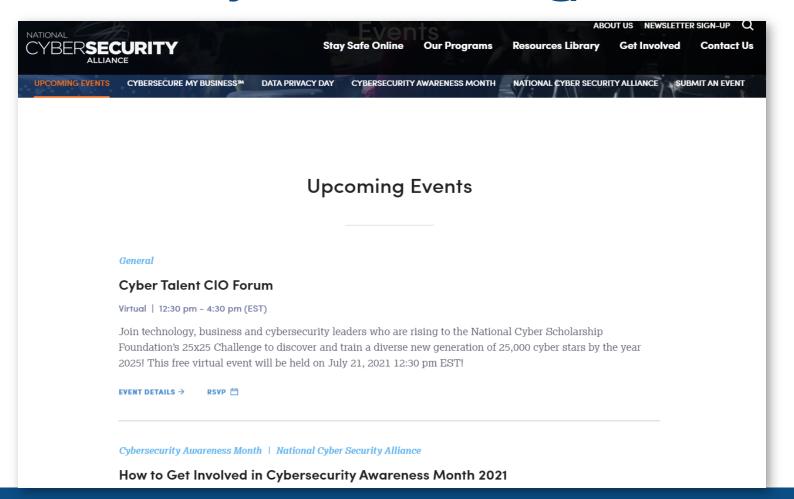
# www.staysafeonline.org/events







# www.staysafeonline.org/events







## References

- DIBNET: www.dibnet.dod.mil
- DCISE: <a href="https://www.dc3.mil/Organizations/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/">https://www.dc3.mil/Organizations/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/</a>
- DOD Cyber Crime Center: <a href="https://www.dc3.mil/Portals/100/Documents/DC3/Resources/Trifolds/DC3-Trifold-Final\_26Apr21.pdf">https://www.dc3.mil/Portals/100/Documents/DC3/Resources/Trifolds/DC3-Trifold-Final\_26Apr21.pdf</a>?ver=rt-N9XYyQMNv4lagCc-4rQ%3d%3d
- CISA: www.CISA.gov/cybersecurity
- STOPRANSOMEWARE.GOV
- NIST: <u>www.csrc.nist.gov</u> or www.nist.gov/smallbusinesscyber
- Center for Internet Security: <a href="www.cisecurity.org/controls">www.cisecurity.org/controls</a>
- 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/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/







# **DAF CISO** webpage

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

