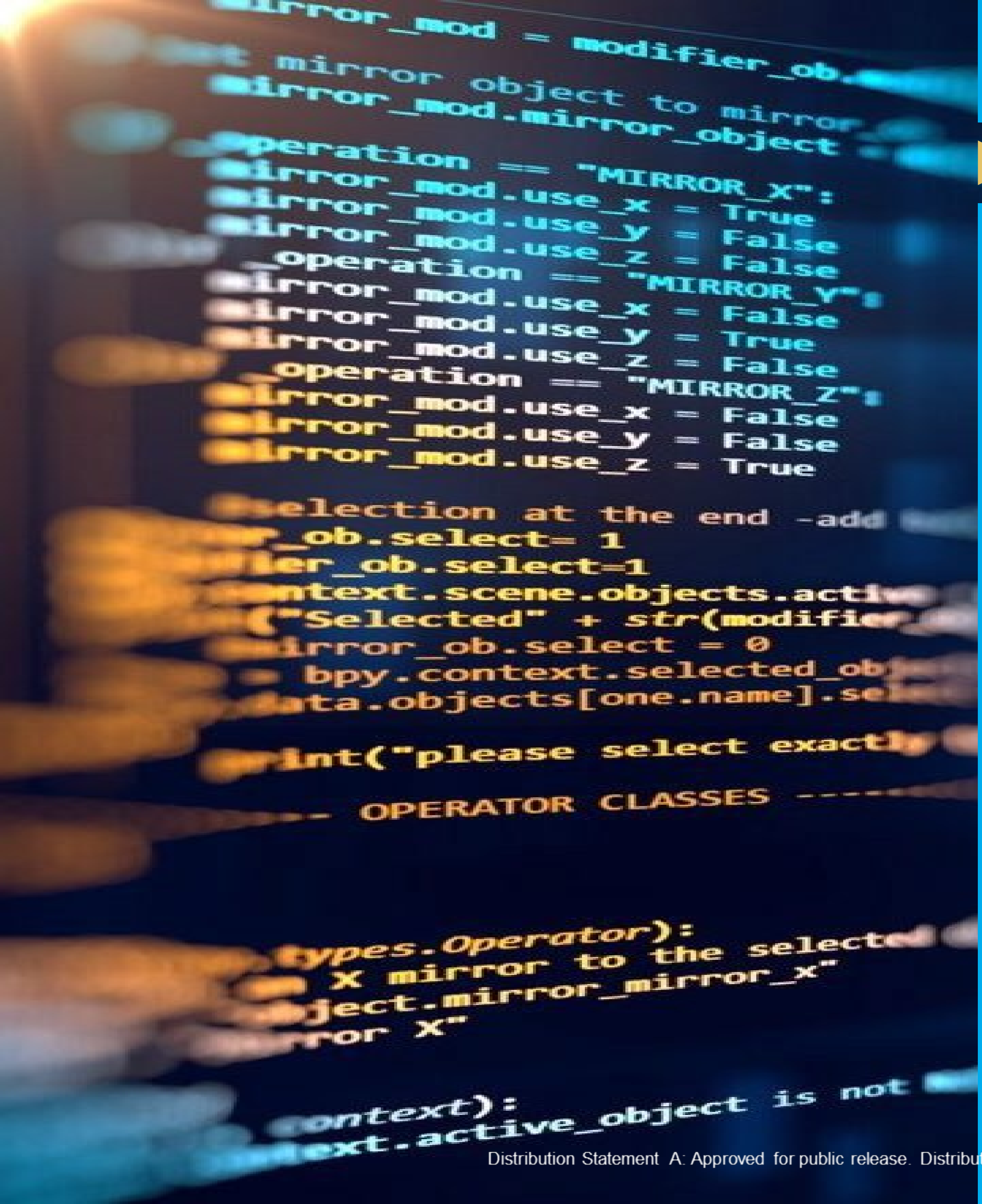


AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's Small Business Cybersecurity Resources Lollapalooza

AFWERX

Jan 30, 2024

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

```
rror_mod = modifier_ob
mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.acti
("Selected" + str(modifie
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactl

- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selecte
ject.mirror_mirror_x"
ror X"

context):
ext.active_object is not
```

AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza

New Mexico APEX Accelerator

Elythia McAnarney

AFWERX

Jan 30, 2024

BLUE CYBER EDUCATION SERIES

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

New Mexico APEX Accelerator

Elythia McAnarney, Procurement Advisor

APEX Accelerator History

Nationally:

- Authorized by congress in 1985 under the Defense Logistics Agency as PTAP
- October 2021, moved management/oversight to the DoD’s Office of Small Business Programs
- Rebranded as APEX Accelerators in November 2022

New Mexico:

- Started in NM in 2009
- Administered/Hosted by the Santa Fe Community College
- Funded by DoD with a match from the state of New Mexico

APEX Accelerators

MISSION: Serve as the axis for existing and new business to strengthen the defense industrial base by accelerating innovation, fostering ingenuity, and establishing resilient and diverse supply chains.

VISION: A diverse and resilient domestic industrial base that can deliver preeminent solutions to the military and other government users

APEX Accelerators are a nationwide network of procurement professionals who help businesses compete for and perform contracts with the DoD, other federal agencies, state & local governments and with government prime contractors.

APEX Accelerators

Who we are:

APEX Accelerators represents 95 centers across the United States. Collectively, APEX Accelerators employ 600 plus procurement counselors who work daily with tens of thousands of businesses, providing them with insights and information on how to best identify, compete for, and win Government contracts.

APEX Accelerators provide contracting assistance – at no cost – in nearly every state plus the District of Columbia and the territories of Puerto Rico and Guam.

Using the link below you can select your state and find the office nearest to you.

https://www.aptac-us.org

How can APEX Accelerator Help you?

Provide:

Assists with vendor registrations and certifications

Help identify government markets and specific contracting opportunities

Assist with bid and proposal preparation

Post-award contract performance

Provide a Bid-Match service (locating bids)

Training and assistance on cybersecurity

New Mexico APEX Accelerator

MISSION:

Counsel, train, and assist New Mexico business owners to obtain government contracts, thereby advancing economic growth in New Mexico

New Mexico APEX Accelerator – Statewide Program

Santa Fe Community College – Main Office

- Statewide Program Manager, Therese Rivera

Albuquerque - CNM/Workforce Training Center

- 2 APEX Advisors + 1 Administrative Assistant
- Elythia McAnarney, Steve Hogan + Tracey Edwards

Albuquerque Hispano Chamber of Commerce

- 1 APEX Advisor – Steve Stewart

Santa Fe – Higher Education Center

- 1 APEX Advisor – Gillis Lang

Las Cruces – Arrowhead Center

- 1 APEX Advisor – Karen Medina

Clovis – located at the SBDC

- 1 APEX Advisor – Jonnie Loadwick

New Mexico APEX Accelerator's Trainings

- We offer no-cost trainings as follows:
  - Introduction to Government Contracting
  - 8(a) Minority Certification Workshop
  - Disaster recovery Procurement Workshop
  - Federal Market Research Workshop
  - How to do business with government agencies (i.e., FEMA, VA, Department of the Navy)
  - **Cybersecurity Requirements for Government Contractors, CMMC**
  - Contract Ready Series (5-parts)
    - I-Understanding Solicitations, II-Proposal Writing, III-Estimating/Pricing,
    - IV-Labor Laws, V-Contract Administration
  - Mentor Protégé
  - And others as needed

New Mexico APEX Accelerator Services

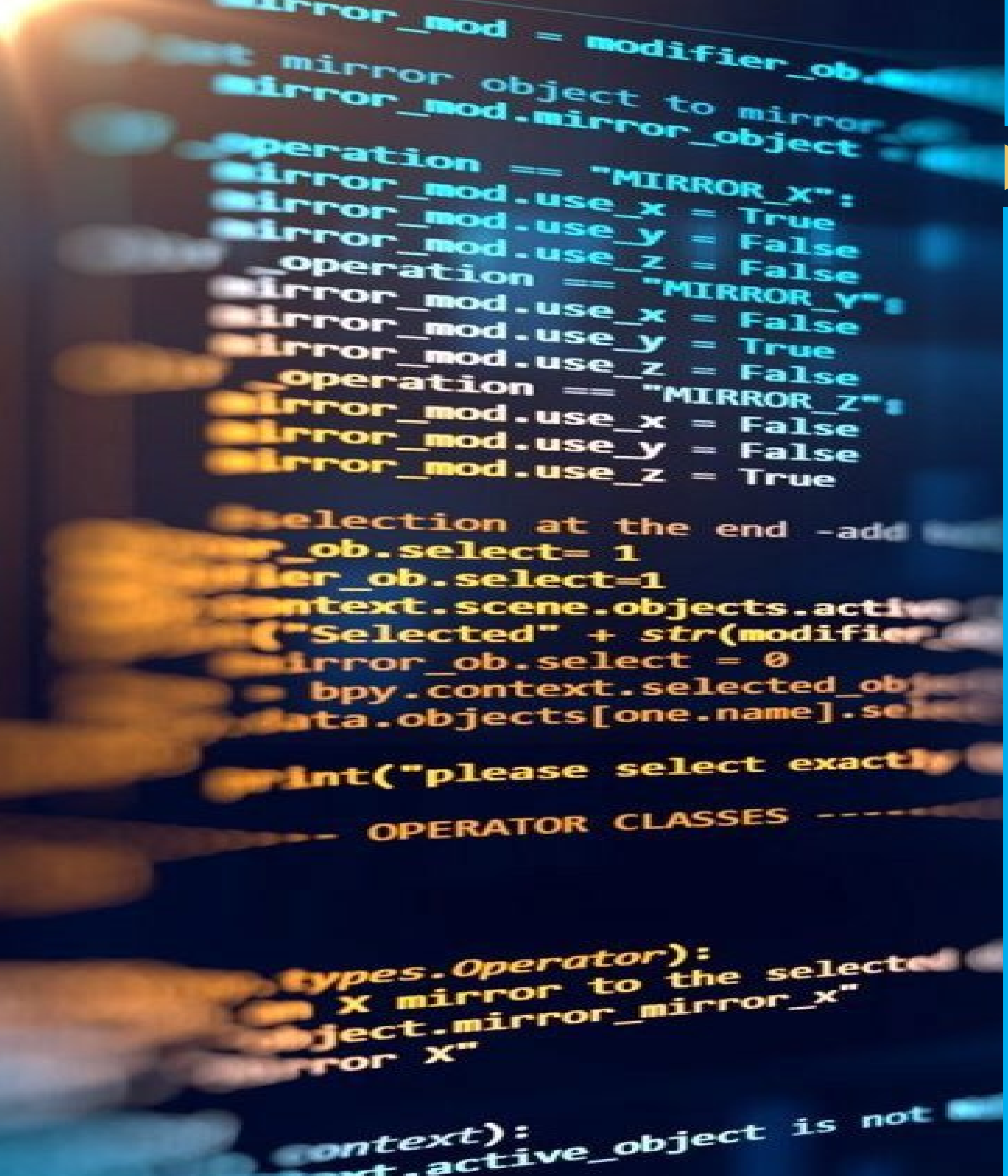
- Other no-cost events include:
  - Matchmaking/Outreach Events
    - Federal
    - State/Local
    - Educational Institutions
    - Prime Contractors
    - Veterans Affairs
  - One-on-one counseling/advising

NEW MEXICO APEX ACCELERATOR

Elythia McAnarney– Procurement Advisor

https://www.nmapexaccelerator.org

This APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense.
NM APEX Accelerator is also funded by the State of New Mexico.



AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza

California
NIST MEP Center
CMTC

Chris Buthe

AFWERX

Jan 30, 2024

BLUE CYBER EDUCATION SERIES

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

Cybersecurity Resources

for U.S. Innovation & Manufacturing

Chris Buthe

CMTC

CMTC

CMTC is affiliated with the National Institute of Standards and Technology (NIST) and is part of the Hollings Manufacturing Extension Partnership (MEP) Program.

CMTC helps California develop and deploy technology, management, and technical expertise to improve small and medium-sized manufacturers and innovators.

CMTC is committed to U.S. manufacturers and innovators that enable our national defense, economic security and public good.

RESOURCE: www.cmtc.com

Your Key Partners are your Resources

Readiness

Capability

Capacity

Success depends on collaboration

Department of Air Force

Blue Cyber Education Series

DAU

DoD DC3

DCSA and CDSE

NIST

NIST MEP National Network

Workforce training organizations

CISA

CISA Critical Manufacturing

RESOURCE: DoD and NIST MEP Resource recommendations

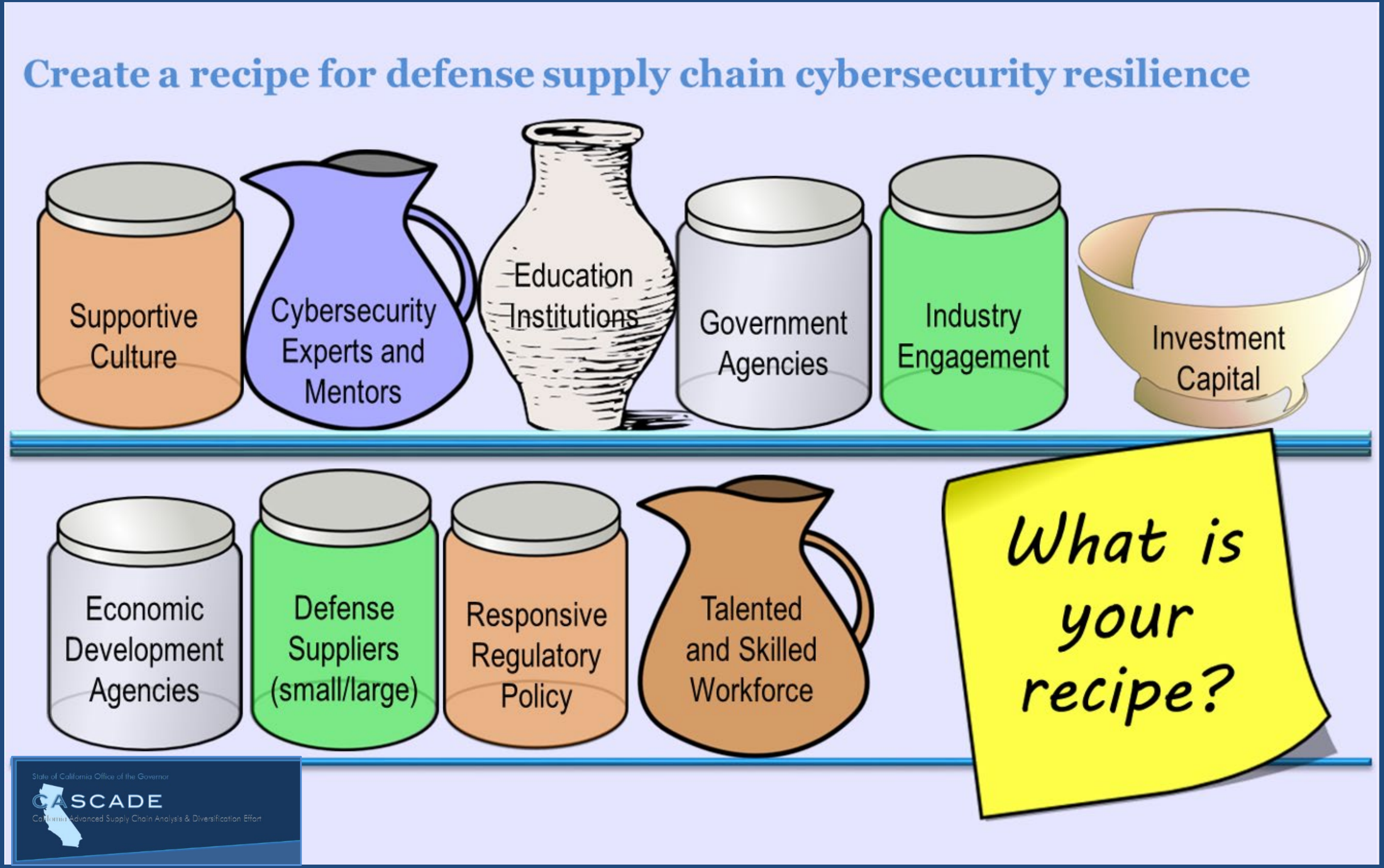
Your Key Partners are your Resources

CMTC California's Manufacturing Network

Readiness

Capability

Capacity


Create a recipe for defense supply chain cybersecurity resilience
Supportive Culture
Cybersecurity Experts and Mentors
Education Institutions
Government Agencies
Industry Engagement
Investment Capital
Economic Development Agencies
Defense Suppliers (small/large)
Responsive Regulatory Policy
Talented and Skilled Workforce
What is your recipe?
State of California Office of the Governor
CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

RESOURCE: https://opr.ca.gov/economic-development/cascade.html

Resources for Innovation Researchers

DAU

U.S. AIR FORCE

CMTC
California's Manufacturing Network

BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

RESOURCE: www.cmtc.com

Resources from MEP National Network

Readiness
Capability
Capacity

MEP National Network™

51 NIST MEP Centers

Collaboration

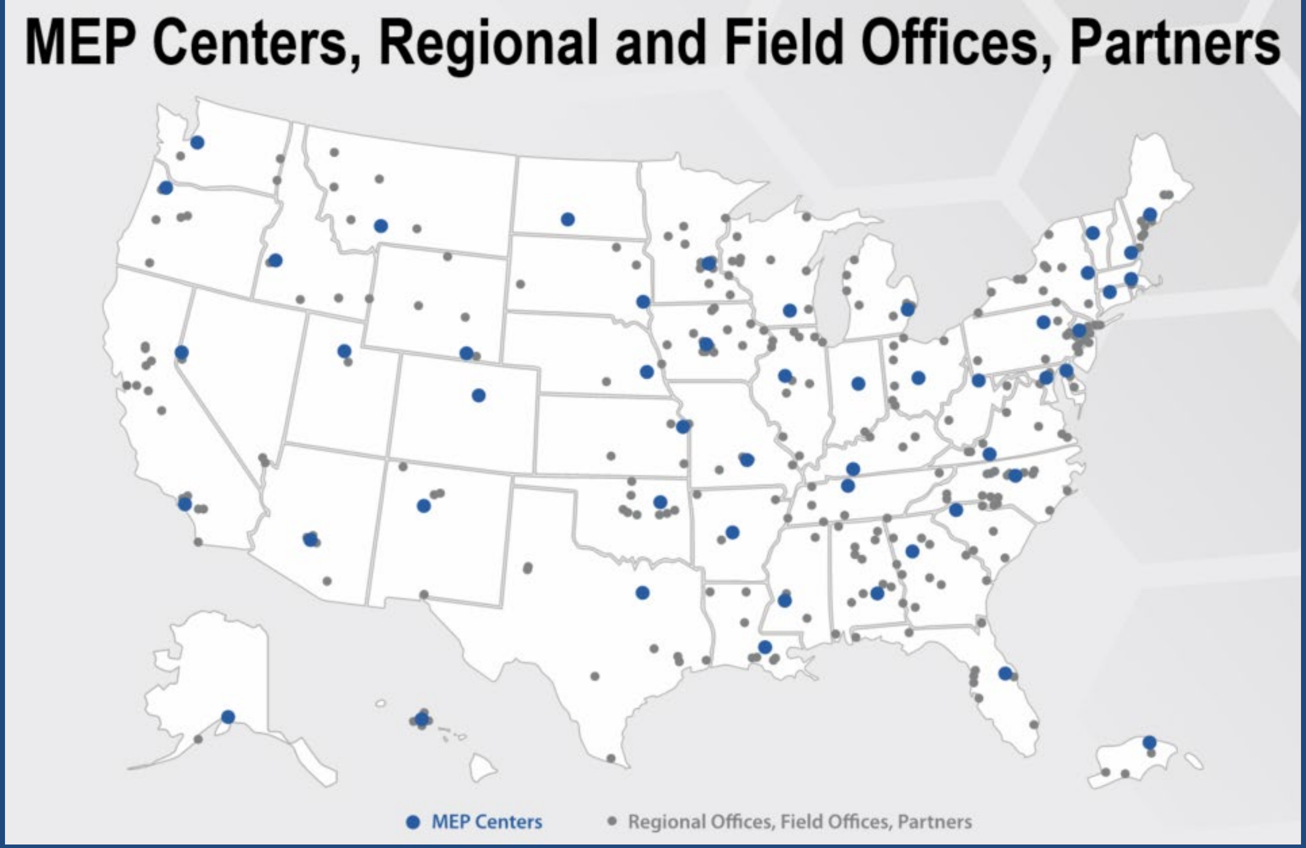
MEP Centers initiate leverage partnerships with other government activities, industry, and academia to foster a collaborative culture

Workforce Training

MEP Centers contribute to workforce training and workforce development to meet long-term strategic needs of small and medium size suppliers

Cybersecurity acumen

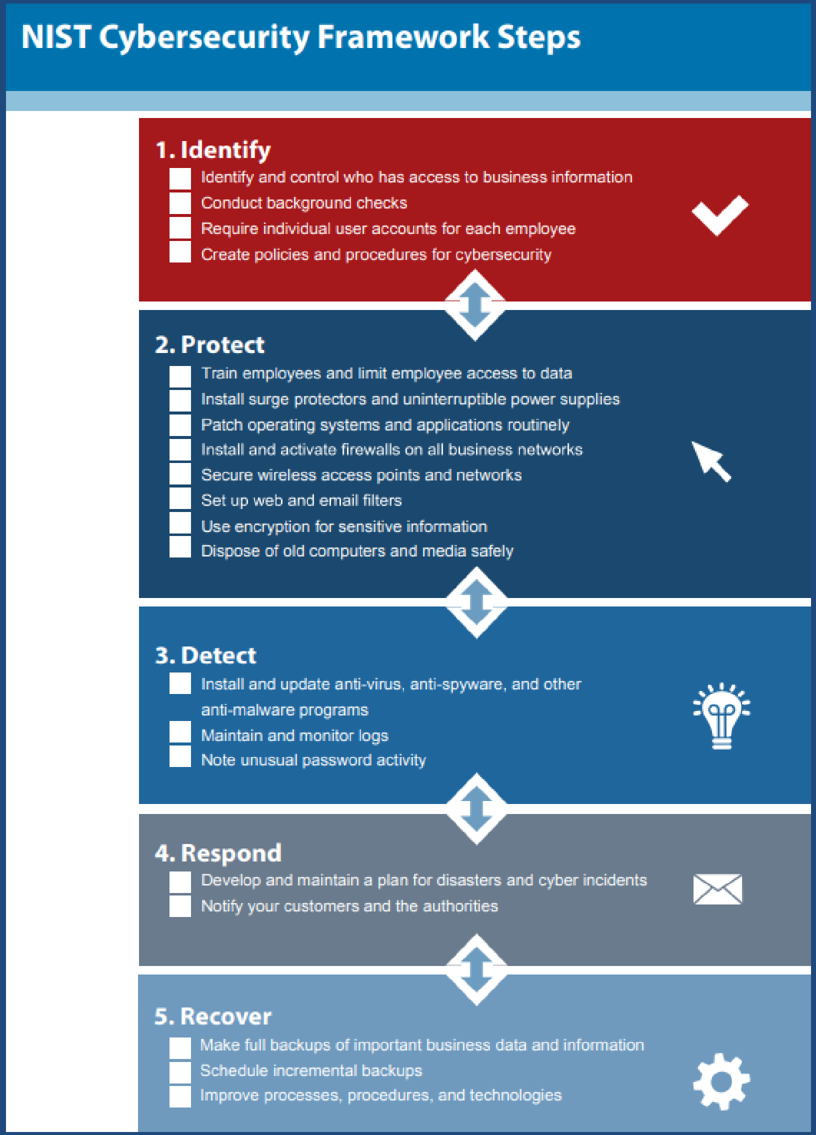
MEP Centers advance cybersecurity acumen, and assist company's access to the necessary tools to support cybersecurity and digital transformation


MEP Centers, Regional and Field Offices, Partners
● MEP Centers
● Regional Offices, Field Offices, Partners

RESOURCE: https://www.nist.gov/mep/mep-national-network

CMTC California's Manufacturing Network

Resources from NIST MEP Centers



NIST Cybersecurity Framework Steps

1. Identify

- □ Identify and control who has access to business information
- □ Conduct background checks
- □ Require individual user accounts for each employee
- □ Create policies and procedures for cybersecurity

2. Protect

- □ Train employees and limit employee access to data
- □ Install surge protectors and uninterruptible power supplies
- □ Patch operating systems and applications routinely
- □ Install and activate firewalls on all business networks
- □ Secure wireless access points and networks
- □ Set up web and email filters
- □ Use encryption for sensitive information
- □ Dispose of old computers and media safely

3. Detect

- □ Install and update anti-virus, anti-spyware, and other anti-malware programs
- □ Maintain and monitor logs
- □ Note unusual password activity

4. Respond

- □ Develop and maintain a plan for disasters and cyber incidents
- □ Notify your customers and the authorities

5. Recover

- □ Make full backups of important business data and information
- □ Schedule incremental backups
- □ Improve processes, procedures, and technologies

Cybersecurity Resilience and Compliance

for applicable Cybersecurity and Privacy Laws and Regulations

NIST SP800-171 rev2

Referenced by DFARS Cybersecurity Provisions & Clauses

Cybersecurity Framework Manufacturing Profile

NISTIR 8183 a roadmap for reducing cybersecurity risk in manufacturing systems

NIST SP800-160 volumes 1 and 2

Volume 1: Systems Security Engineering

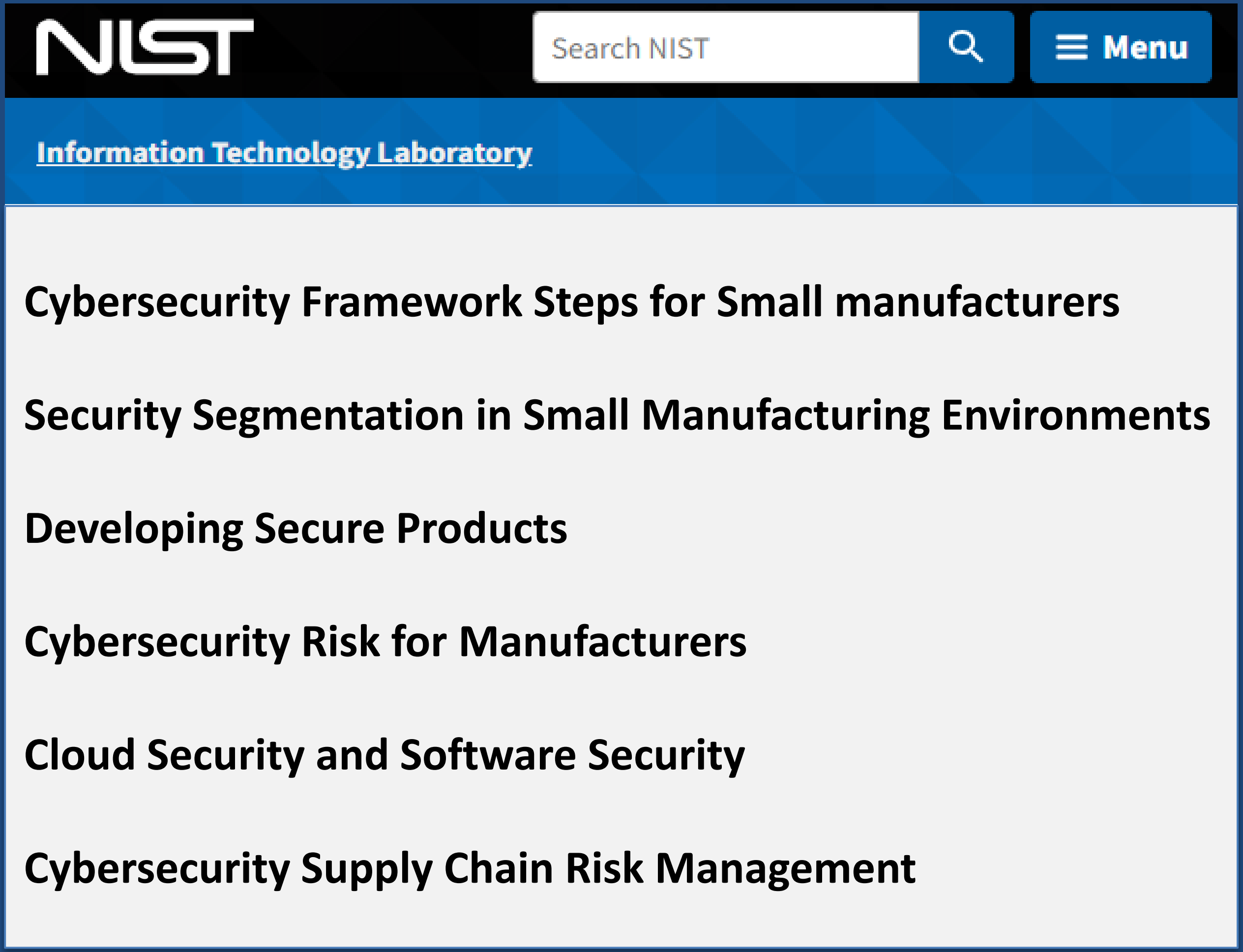
Volume 2: Developing Cyber-Resilient Systems

RESOURCE: https://www.nist.gov/mep/cybersecurity-resources-manufacturers

Resources from your NIST Laboratories

Readiness
Capability
Capacity

CMTC
California's Manufacturing Network



Cybersecurity Framework Steps for Small manufacturers

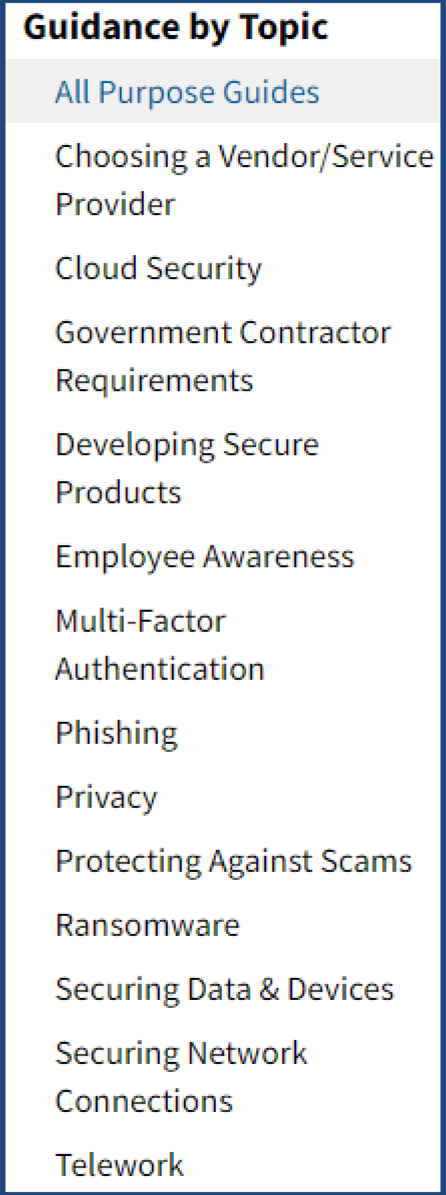
Security Segmentation in Small Manufacturing Environments

Developing Secure Products

Cybersecurity Risk for Manufacturers

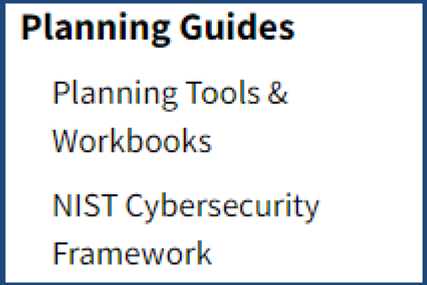
Cloud Security and Software Security

Cybersecurity Supply Chain Risk Management



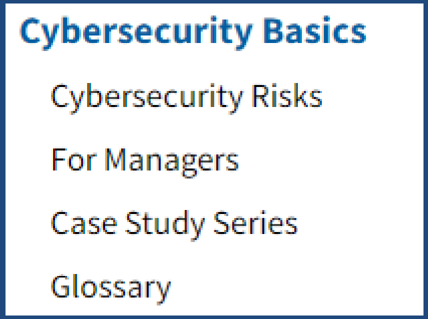
Guidance by Topic

- All Purpose Guides
- Choosing a Vendor/Service Provider
- Cloud Security
- Government Contractor Requirements
- Developing Secure Products
- Employee Awareness
- Multi-Factor Authentication
- Phishing
- Privacy
- Protecting Against Scams
- Ransomware
- Securing Data & Devices
- Securing Network Connections
- Telework



Planning Guides

- Planning Tools & Workbooks
- NIST Cybersecurity Framework



Cybersecurity Basics

- Cybersecurity Risks
- For Managers
- Case Study Series
- Glossary

RESOURCE: https://www.nist.gov/itl/smallbusinesscyber

Resources from CMTC CyberTeam

NIST SP800-171 rev2 Training and Technical Assistance

Cost Effective Cybersecurity

Security Reference Architecture

Managing the Security Practices of IT Service Providers & MSPs

Ransomware Readiness Assessment

Managing the Security Practices of IT service providers & MSPs

- May be part of a cost-effective implementation
- Addresses lack of visibility into third party cybersecurity service delivery and responsibilities
- Improves a company’s oversight practices to manage their third party service provider

TLP:WHITE

JOINT
CYBERSECURITY
ADVISORY

Product ID: AA22-131A

May 11, 2022

Co-authored by:

National Cyber Security Centre a part of GCHQ | ACSC Australian Cyber Security Centre | Communications Security Establishment Canadian Centre for Cyber Security | Centre de la sécurité des télécommunications Centre canadien pour la cybersécurité | Government Communications Security Bureau Te Tira Tiaki

Protecting Against Cyber Threats to Managed Service Providers and their Customers

SUMMARY

The cybersecurity authorities of the United Kingdom (NCSC-UK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ), and the United States (CISA), (NSA), (FBI) are aware of recent reports that observe an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue.[1] This joint Cybersecurity Advisory (CSA) provides actions MSPs and their customers can take to reduce their risk of falling victim to a cyber intrusion.

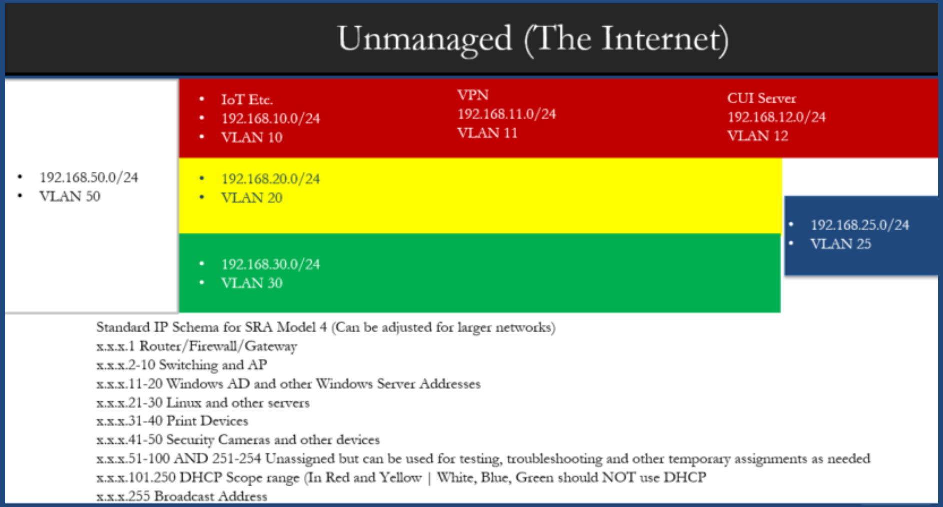
This advisory describes cybersecurity best practices for information and communications technology (ICT) services and functions, focusing on guidance that enables transparent discussions between MSPs and their customers on securing sensitive data. Organizations should implement these guidelines as appropriate to their unique environments, in accordance with their specific security needs, and in compliance with applicable regulations. MSP customers should verify that the contractual arrangements with their provider include cybersecurity measures in line with their particular security requirements.

Tactical actions for MSPs and their customers to take today:

- Identify and disable accounts that are no longer in use.
- Enforce MFA on MSP accounts that access the customer environment and monitor for unexplained failed authentication.
- Ensure MSP-customer contracts transparently identify ownership of ICT security roles and responsibilities.

CMTC Security Reference Architecture(s)

- May be part of a cost-effective cybersecurity implementation
- Addresses vulnerabilities in flat networks
- Improves security of valuable information and assets



Unmanaged (The Internet)

- IoT Etc.
- 192.168.10.0/24
- VLAN 10

VPN
192.168.11.0/24
VLAN 11

CUI Server
192.168.12.0/24
VLAN 12

- 192.168.50.0/24
- VLAN 50

- 192.168.20.0/24
- VLAN 20

- 192.168.25.0/24
- VLAN 25

- 192.168.30.0/24
- VLAN 30

Standard IP Schema for SRA Model 4 (Can be adjusted for larger networks)
x.x.x.1 Router/Firewall/Gateway
x.x.x.2-10 Switching and AP
x.x.x.11-20 Windows AD and other Windows Server Addresses
x.x.x.21-30 Linux and other servers
x.x.x.31-40 Print Devices
x.x.x.41-50 Security Cameras and other devices
x.x.x.51-100 AND 251-254 Unassigned but can be used for testing, troubleshooting and other temporary assignments as needed
x.x.x.101.250 DHCP Scope range (In Red and Yellow | White, Blue, Green should NOT use DHCP
x.x.x.255 Broadcast Address

Resources from CMTC CyberTeam

CMTC Security Reference Architecture(s) provide an extensible & scalable framework to support the following requirements:

- CMMC CM.3.068 / NIST SP800-171r2 Requirement 3.4.7
  - Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
- CMMC SC.3.180 / NIST SP800-171r2 Requirement 3.13.2
  - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
- CMMC SC.3.183 / NIST SP800-171r2 Requirement 3.13.6
  - Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

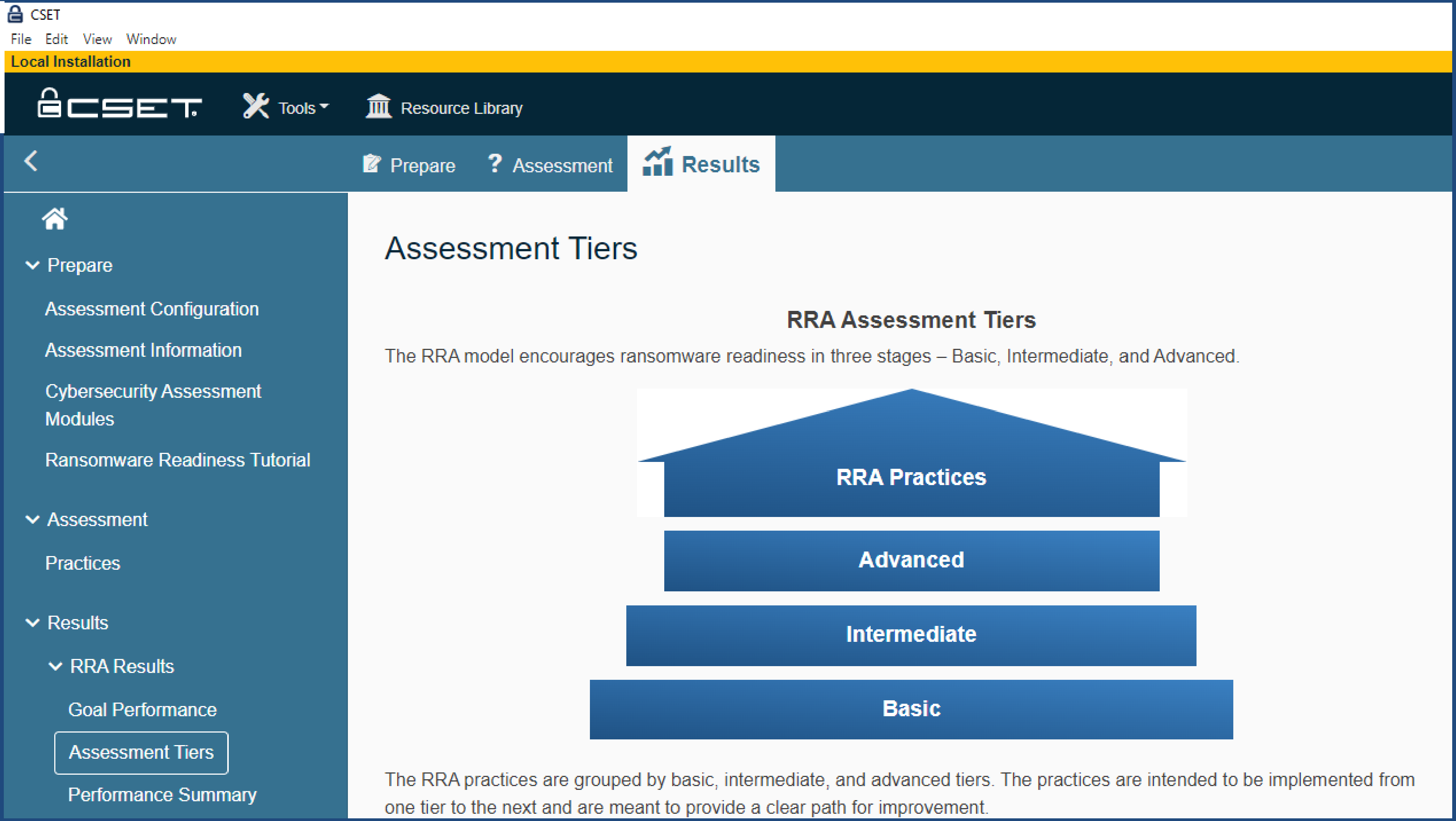
Resources from CMTC CyberTeam

Readiness
Capability
Capacity

CMTC California's Manufacturing Network

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CSET Ransomware Readiness Assessment



Assessment Tiers

RRA Assessment Tiers

The RRA model encourages ransomware readiness in three stages – Basic, Intermediate, and Advanced.

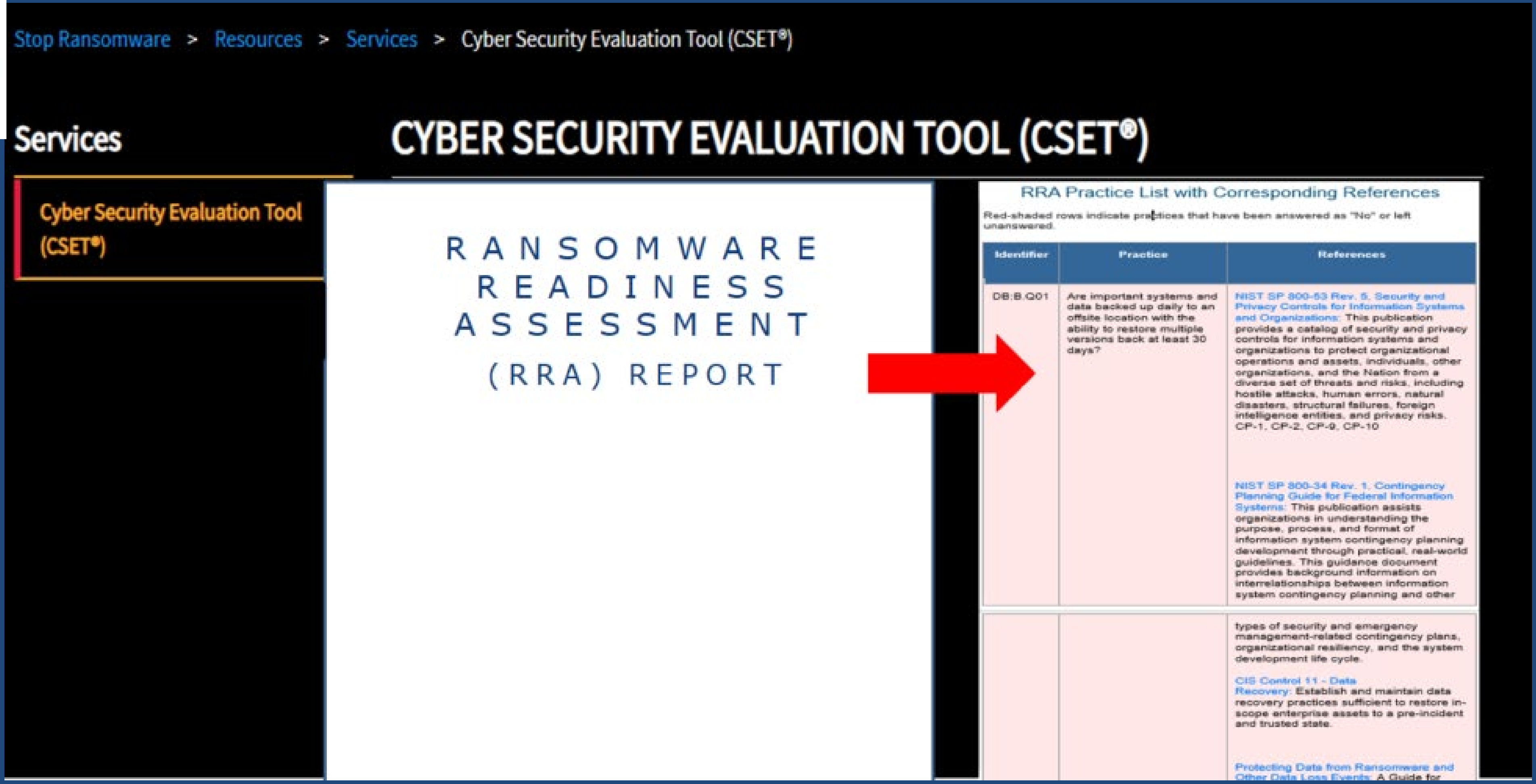
The RRA practices are grouped by basic, intermediate, and advanced tiers. The practices are intended to be implemented from one tier to the next and are meant to provide a clear path for improvement.

RESOURCE: https://cset-download.inl.gov/.

Resources from CMTC CyberTeam

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CSET Ransomware Readiness Assessment



Stop Ransomware > Resources > Services > Cyber Security Evaluation Tool (CSET®)

Services

Cyber Security Evaluation Tool (CSET®)

CYBER SECURITY EVALUATION TOOL (CSET®)

RANSOMWARE READINESS ASSESSMENT (RRA) REPORT

RRA Practice List with Corresponding References

Red-shaded rows indicate practices that have been answered as "No" or left unanswered.

Identifier	Practice	References
DB:B.Q01	Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days?	NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-1, CP-2, CP-9, CP-10 NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. CIS Control 11 - Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state. Protecting Data from Ransomware and Other Data Loss Events: A Guide for

RESOURCE: https://cset-download.inl.gov/.

Resources from CADENCE & CASCADE

Readiness
Capability
Capacity

CADENCE
California Advanced Defense Ecosystems & National Consortia Effort

5G
CADENCE
California Advanced Defense Ecosystems & National Consortia Effort

SECURITY
CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

CADENCE and CASCADE are initiatives funded by the U.S. Department of Defense to bolster California's defense ecosystems & supply chain resilience.

California Governor's Office of Planning & Research

- ETP California Employment Training Panel
- CMTC
- El Camino Community College
- California Community College System
- Cal Poly San Luis Obispo
- San Diego East County Economic Development Center
- San Diego Cyber Center of Excellence
- **Next Flex**: Flexible Hybrid Electronics Manufacturing Institute

RESOURCE: https://opr.ca.gov/planning/land-use/military-affairs/cadence.html RESOURCE: https://opr.ca.gov/economic-development/cascade.html

CMTC
California's Manufacturing Network

Resources from CADENCE

5G
CADENCE
California Advanced Defense Ecosystems & National Consortia Effort

CADENCE

- Defense Critical Technology Ecosystems
- Microelectronics
- Flexible Hybrid Electronics
- Space Commercialization & Manufacturing
- Future G and 5G technologies
- AI & Machine Learning
- Joint All-Domain Command & Control (JADC2)
- Converging Technology Platforms

RESOURCE: https://opr.ca.gov/planning/land-use/military-affairs/cadence.html

Resources from CADENCE

Readiness
Capability
Capacity

5G
CADENCE
California Advanced Defense Ecosystems & National Consortia Effort

CADENCE

- DFARS cybersecurity assessments
- NIST cybersecurity implementation training
- Zero Trust training
- OpSec Threat Situational Awareness
- Innovation Protection Planning
- Cyber Workforce Development
- Smart Manufacturing Workforce Development
- Critical Technology Manufacturing Skills
- Engineering and Manufacturing Support for Flexible Hybrid Electronics Development

RESOURCE: https://opr.ca.gov/planning/land-use/military-affairs/cadence.html

Resources from CASCADE

SECURITY
CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

CASCADE

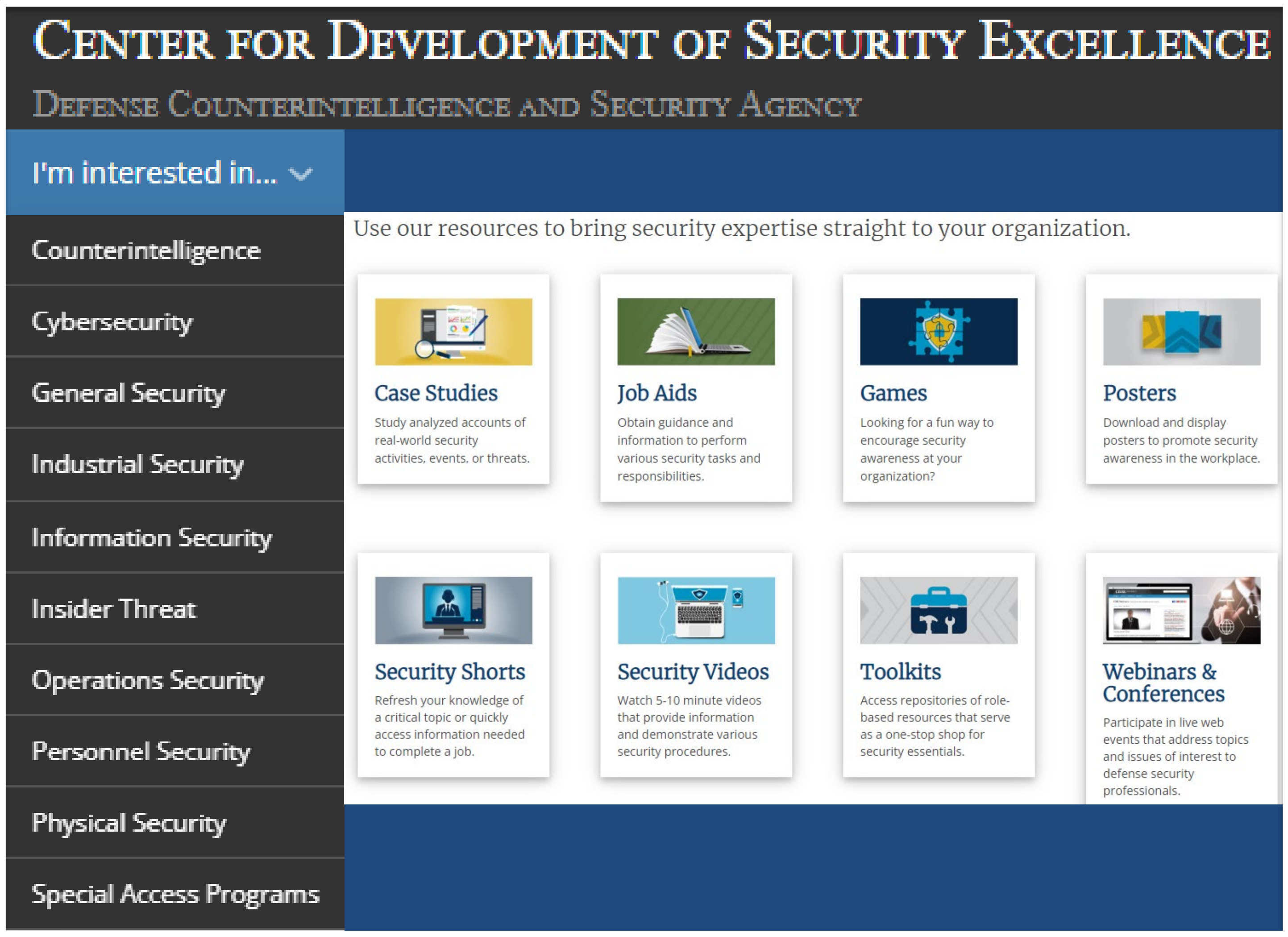
- Defense Critical Priorities
- Defense Ecosystem Resilience
- DFARS Cybersecurity Compliance
- Space and Cybersecurity Operations
- Cybersecurity Skills Upgrading support
- Cyber Workforce Development
- SBIR/STTR Cybersecurity Internships
- Cyber Job Placements
- Collaboration with APEX Accelerators (PTAC)

RESOURCE: https://opr.ca.gov/economic-development/cascade.html

Resources from DCSA and CDSE

Defense Counterintelligence and Security Agency

Controlled Unclassified Information (CUI)



CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Use our resources to bring security expertise straight to your organization.

Case Studies
Study analyzed accounts of real-world security activities, events, or threats.

Job Aids
Obtain guidance and information to perform various security tasks and responsibilities.

Games
Looking for a fun way to encourage security awareness at your organization?

Posters
Download and display posters to promote security awareness in the workplace.

Security Shorts
Refresh your knowledge of a critical topic or quickly access information needed to complete a job.

Security Videos
Watch 5-10 minute videos that provide information and demonstrate various security procedures.

Toolkits
Access repositories of role-based resources that serve as a one-stop shop for security essentials.

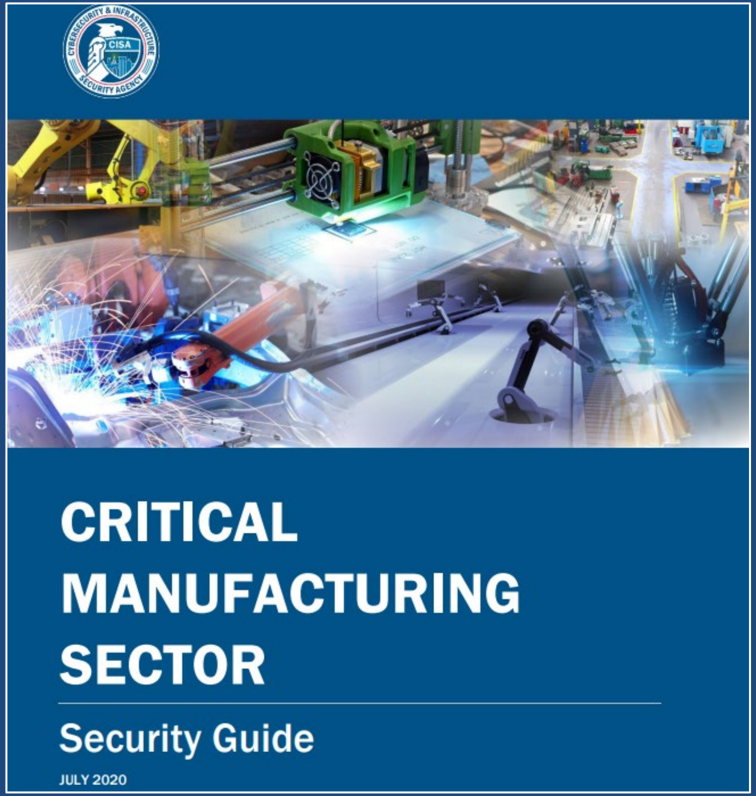
Webinars & Conferences
Participate in live web events that address topics and issues of interest to defense security professionals.

RESOURCE: DCSA https://www.dcsa.mil/Industrial-Security/Controlled-Unclassified-Information-CUI/ RESOURCE: CDSE https://www.cdse.edu

Resources from CISA

Readiness
Capability
Capacity

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



CRITICAL MANUFACTURING SECTOR

Security Guide

JULY 2020

SECURING THE SOFTWARE SUPPLY CHAIN

RECOMMENDED PRACTICES GUIDE FOR SUPPLIERS

Enduring Security Framework
September 2022

DON'T WAKE UP TO A RANSOMWARE ATTACK

CISA

Learning Objectives

Terminal Objective
Understand the fundamentals of ransomware and the impact it can have on your organization

Enabling Objectives

- Define ransomware
- Be able to identify signs of a ransomware attack
- Learn mitigation steps of ransomware attacks
- Understand how to recover from a ransomware attack
- Understand impacts of ransomware attacks though case studies

CISA

RESOURCE: https://www.cisa.gov/shields-up

Resources: CMTC 12 Actions to Take

Cybersecurity Deficit	Implement NIST SP800-171
Cybersecurity Resilience	Use CSET Ransomware Readiness Review
Defend your Access Points	Manage 3rd Party Providers
Deny Adversaries Opportunity	Train employees on Threat Situational Awareness
Operations Security	Use CDSE no cost security training
Beware of Insertion of Unknowns	Read Deliver Uncompromised
EAR and ITAR processes	Update EAR and ITAR processes with Entities List
SHIELDS UP	Use CISA Critical Manufacturing Security Guide
Supply Chain Risk Management	Use CISA Supply Chain ESSENTIALS tools
Check Vulnerabilities	Use CISA Common Vulnerabilities & Exposures
Threat Information	Subscribe to Cyber Advisories
Define your Resilience	Use Center for Strategic & International Studies

RESOURCE: www.cmtc.com

Thank you,

CMTC
California's Manufacturing Network

California Manufacturing Technology Consulting
3760 Kilroy Airport Way, Suite 450,
Long Beach, California 90806-2455
310.263.3060 www.cmtc.com

Email: info@cmtc.com

DAU

DEPARTMENT OF THE NAVY
SBIR
STTR
Small Business Innovation Research

MEP
National
Network™

BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza

National Security Agency Defense Industrial Base Services

Peter DeLuca

AFWERX

Jan 30, 2024

BLUE CYBER EDUCATION SERIES

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

NSA CYBERSECURITY

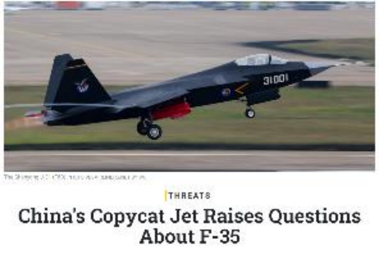
NSA's DIB Cybersecurity Services

NSA CYBERSECURITY COLLABORATION CENTER
2024

THE THREAT LANDSCAPE

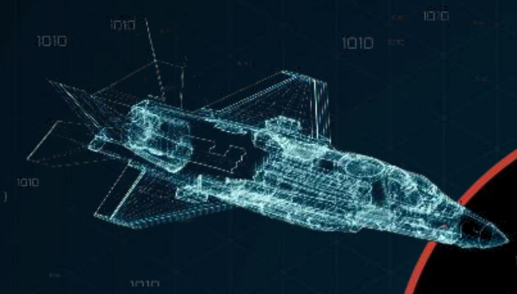
Nation-states Target Primes & SMBs

Nation-states are Leveraging U.S. based infrastructure to obfuscate activities



THREATS

China's Copycat Jet Raises Questions About F-35



Ransomware

Disproportionately impacts SMBs

In 2021 **81%** of ransomware attacks were against companies with fewer than 1,000 employees.

55% of consumers in the U.S. would be less likely to continue doing business with companies that are breached.

Exploitation of Internet-facing, publicly known vulnerabilities are the most common attack vector for ransomware

Complexity of the DoD Supply Chain

How Many Contacts Are Truly In Your Network?

25	Prime companies
18,476	Tier two subs
229,562	Tier three subs

Patch Fatigue & Issue Prioritization

Projected **500** CVEs published per week in 2025

The average org has **>100,000** **backlogged** vulnerabilities

~25,000 Published in NVD in 2022 – Less than **2%** were exploited by malicious actors

Malicious actors **weaponize vulnerabilities** 40% faster than defenders remediate them and most organizations **remediate less than half of** known vulnerabilities.

What do you plan to do differently for vulnerability management by 2025? What are you doing now that needs bolstering?

THREAT-INFORMED DEFENSE

SIGNALS INTELLIGENCE

CYBERSECURITY

NSA's goal is to be the "signal through the noise" for the Defense Industrial Base

NSA Cybersecurity Collaboration Center

INFORMED BY NSA INTEL

UNCLASSIFIED ENGAGEMENTS

EMPOWERING “BEST-OF-BREED” COMPANIES

FREE CYBERSECURITY SERVICES FOR SMBs

Operationalizing Intelligence, Implementing the National Cybersecurity Strategy, and Protecting the DIB Ecosystem

Our Partners

400+ voluntary partners at every level of the DIB ecosystem.

All partnerships underpinned by an NDA, based on mutual benefit and trust

DIB PRIMES

DIB primes cover **80% of DoD acquisition spending**

DIB SERVICE PROVIDERS

IT and cybersecurity companies that **reach billions of endpoints**

DIB SMBs

DIB SMBs that support critical DoD programs

Our Cybersecurity Services

Designed to protect against the primary methods that adversaries are weaponizing against the DIB

Endorsed and Paid For by DoD CIO

Supports NIST 800-171 requirements

Provided through third parties (competitively awarded contracts)

Low barrier for entry: Active DoD contract (sub or prime) OR access to non-public DoD information

Bolstered by NSA threat intel

Our Core Services

& how they support NIST 800-171 controls

PROTECTIVE DNS (DNS FILTER)

NIST 800-171
System & Information Integrity
3.14.06

ATTACK SURFACE MANAGMENT

NIST 800-171
Risk Assessment
3.11.02, 3.11.03

THREAT INTELLIGENCE COLLABORATION

NIST 800-171
System & Information Integrity
3.14.03

Upcoming pilots include cloud security, threat hunting, phishing protection, and autonomous penetration testing

What does NSA get out of this?

- Secure warfighter (data, comms, weapons, etc.)
- Proprietary tech is protected, ensuring national security and economic advantage
- We understand how our adversaries are targeting the networks we care about the most (greater insights)
- We impact our adversaries’ cyber operations – with ripple effects
- We help SMBs below the “cyber poverty line”

What do you get out of this?

- Free stuff ☺
- Improved cyber hygiene
- Improved protection of your proprietary information
- Reduce risk of becoming a victim to a costly incident
- Support on your CMMC journey
- Access to additional cybersecurity pilots down the road

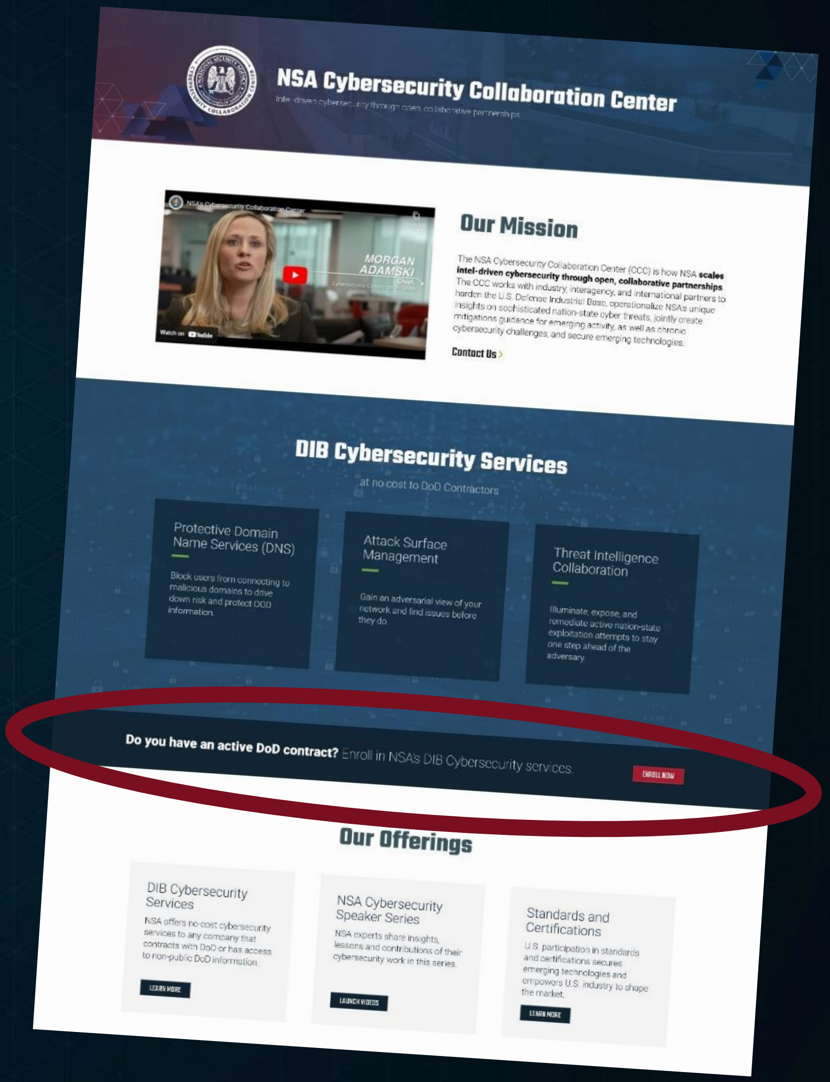
CALL TO ACTION: ENROLL & TELL YOUR FRIENDS

"Get Started"
www.nsa.gov/ccc

Eligibility
Confirmation

Sign
Agreement

Services
Enrollment



NSA Cybersecurity Collaboration Center

Intel-driven cybersecurity through open, collaborative partnerships

NSA's Cybersecurity Collaboration Center
MORGAN ADAMSKI
Chief, Cybersecurity Collaboration Center
Watch on YouTube

Our Mission

The NSA Cybersecurity Collaboration Center (CCC) is how NSA **scales intel-driven cybersecurity through open, collaborative partnerships**. The CCC works with industry, interagency, and international partners to harden the U.S. Defense Industrial Base, operationalize NSA's unique insights on sophisticated nation-state cyber threats, jointly create mitigations guidance for emerging activity, as well as chronic cybersecurity challenges, and secure emerging technologies.

Contact Us >

DIB Cybersecurity Services

at no cost to DoD Contractors

Protective Domain Name Services (DNS)

Block users from connecting to malicious domains to drive down risk and protect DOD information.

Attack Surface Management

Gain an adversarial view of your network and find issues before they do.

Threat Intelligence Collaboration

Illuminate, expose, and remediate active nation-state exploitation attempts to stay one step ahead of the adversary.

Do you have an active DoD contract? Enroll in NSA's DIB Cybersecurity services.

Our Offerings

DIB Cybersecurity Services

NSA offers no-cost cybersecurity services to any company that contracts with DoD or has access to non-public DoD information.

NSA Cybersecurity Speaker Series

NSA experts share insights, lessons and contributions of their cybersecurity work in this series.

Standards and Certifications

U.S. participation in standards and certifications secures emerging technologies and empowers U.S. industry to shape the market.

In some cases, this process can take less than 15 minutes

DIB_DEFENSE@cyber.nsa.gov

www.NSA.gov/CCC

@NSAcyber

AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza

NIST Small Business Corner

Daniel Eliot

AFWERX

Jan 30, 2024

BLUE CYBER EDUCATION SERIES

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

Overview of NIST Small Business Resources

January 30, 2024

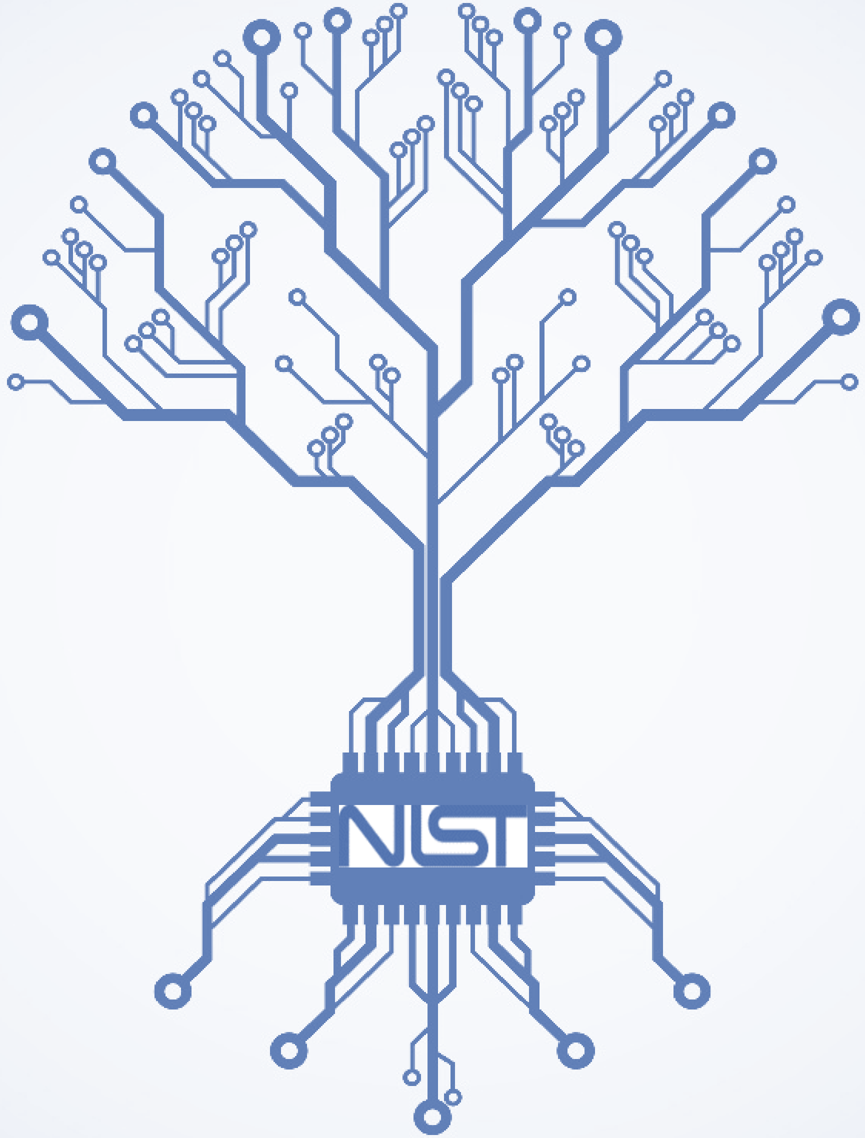
NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Celebrating 50+ Years in Cybersecurity

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

We **cultivate trust** by advancing cybersecurity & privacy **standards & guidelines**, **technology**, & **measurement science**.

nist.gov



Agenda

- NIST Small Business Cybersecurity Corner Website
- Hollings Manufacturing Extension Partnership (MEP)
- NIST Small Business Innovation Research (SBIR) Program
- Additional Resources

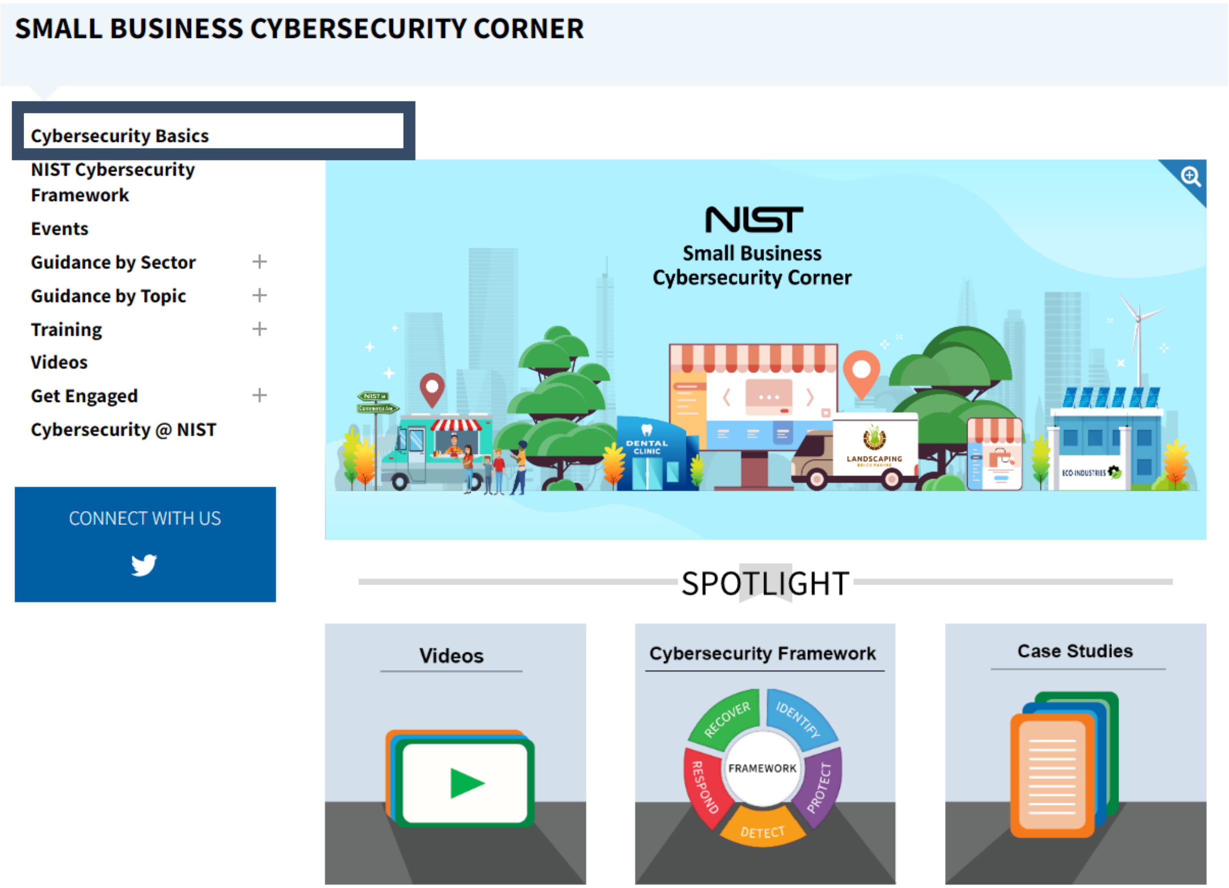
NIST Small Business Cybersecurity Corner

Your secure business is just around the corner.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

www.nist.gov/itl/smallbusinesscyber

Cybersecurity Basics



SMALL BUSINESS CYBERSECURITY CORNER

- Cybersecurity Basics
- NIST Cybersecurity Framework
- Events
- Guidance by Sector +
- Guidance by Topic +
- Training +
- Videos
- Get Engaged +
- Cybersecurity @ NIST

CONNECT WITH US

SPOTLIGHT

Videos

Cybersecurity Framework

Case Studies

https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics

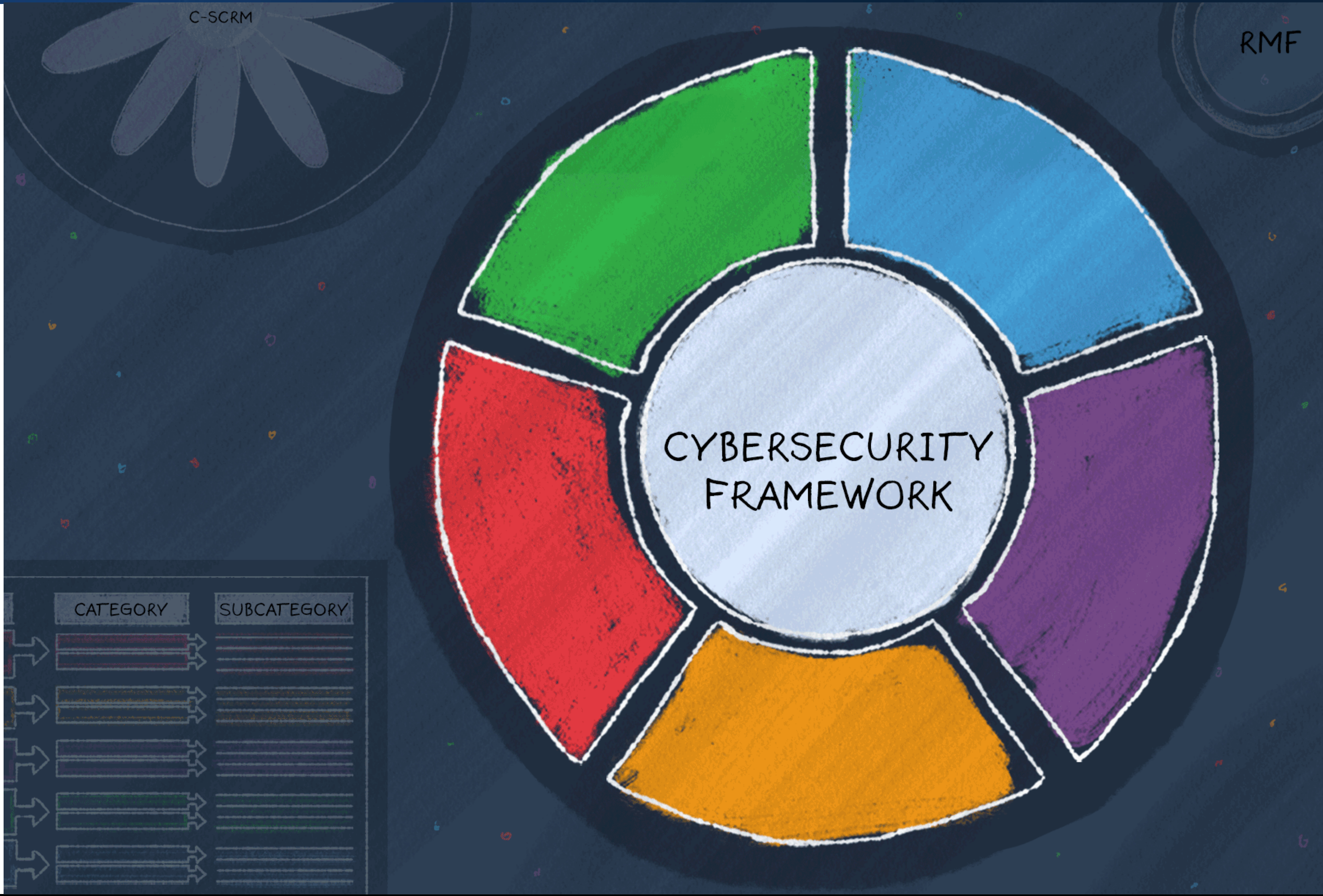
- Understand that cyber threats are a business risk, and having strong cybersecurity is a competitive advantage.
- Enable multi-factor authentication on all accounts that offer it.
- Require strong passwords and consider using a password manager.
- Change default manufacturer passwords.
- Install and maintain updated antivirus software.
- Update and patch all software when new versions are available.
- Learn how to protect your business from phishing.
- Train employees on basic cybersecurity hygiene.

NIST Cybersecurity Framework (CSF)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

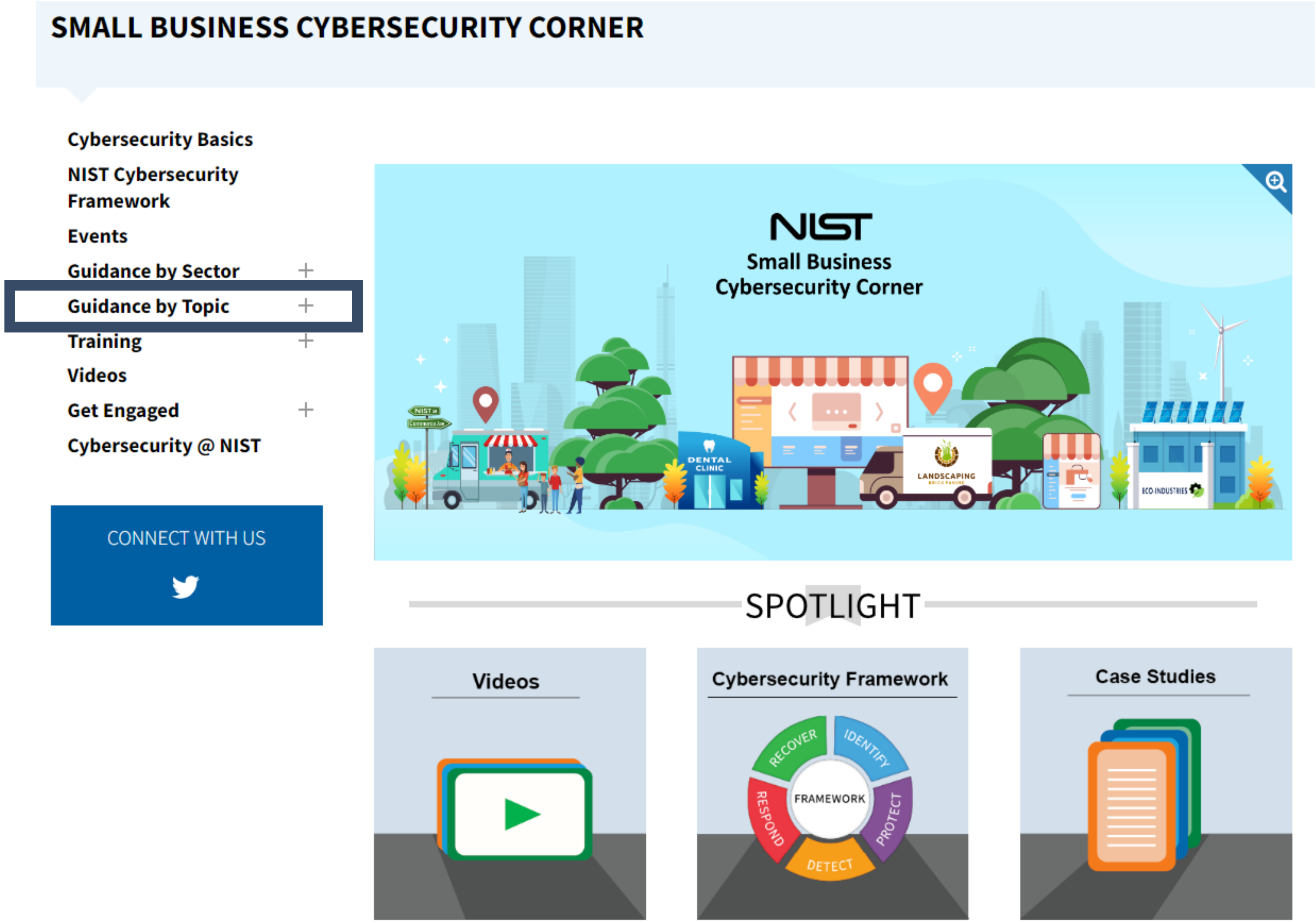
CSF Introductory Resources

- NIST's Cybersecurity Framework Quick Start Guide
- MEP's Cybersecurity Framework Steps for Small Manufacturers
- FTC's Understanding the NIST Cybersecurity Framework



www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework

Guidance by Topic



SMALL BUSINESS CYBERSECURITY CORNER

- Cybersecurity Basics
- NIST Cybersecurity Framework
- Events
- Guidance by Sector +
- Guidance by Topic +
- Training +
- Videos
- Get Engaged +
- Cybersecurity @ NIST

CONNECT WITH US

NIST Small Business Cybersecurity Corner

SPOTLIGHT

Videos

Cybersecurity Framework

Case Studies

- ✓ All-Purpose Guides
- ✓ Choosing A Service Provider
- ✓ Cloud Security
- ✓ Cybersecurity Insurance
- ✓ Government Contractor Requirements
- ✓ Developing Secure Products
- ✓ Employee Awareness
- ✓ Multi-Factor Authentication
- ✓ Phishing
- ✓ Privacy
- ✓ Protecting Against Scams
- ✓ Ransomware
- ✓ Responding to a Cyber Incident
- ✓ Securing Data and Devices
- ✓ Securing Network Connections
- ✓ Telework

Short Videos

Phishing

Protecting Your Small Business: Ph…
Protecting Your Small Business:
Phishing

See the Phishing companion PDF here.

Multi-Factor Authentication

Protecting Your Small Business: M…
Protecting Your Small Business:
Multi-Factor Authentication

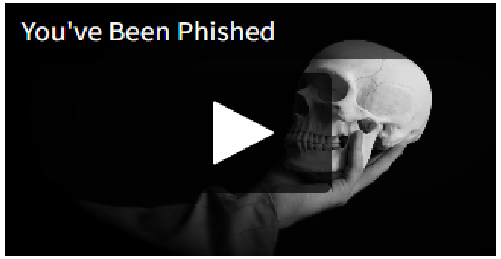
See the Multi-Factor Authentication companion PDF here.

Ransomware

Protecting Your Small Business: Ra…
Protecting Your Small Business:
Ransomware

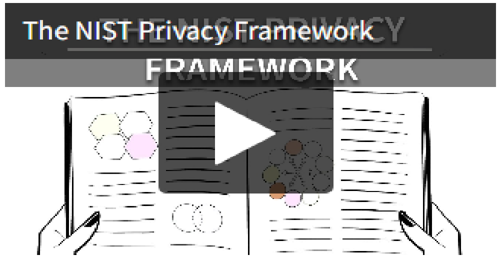
See the Ransomware companion PDF here.

You've Been Phished



NIST research has uncovered one reason, and the findings could help CIOs mount a better defense.

The NIST Privacy Framework

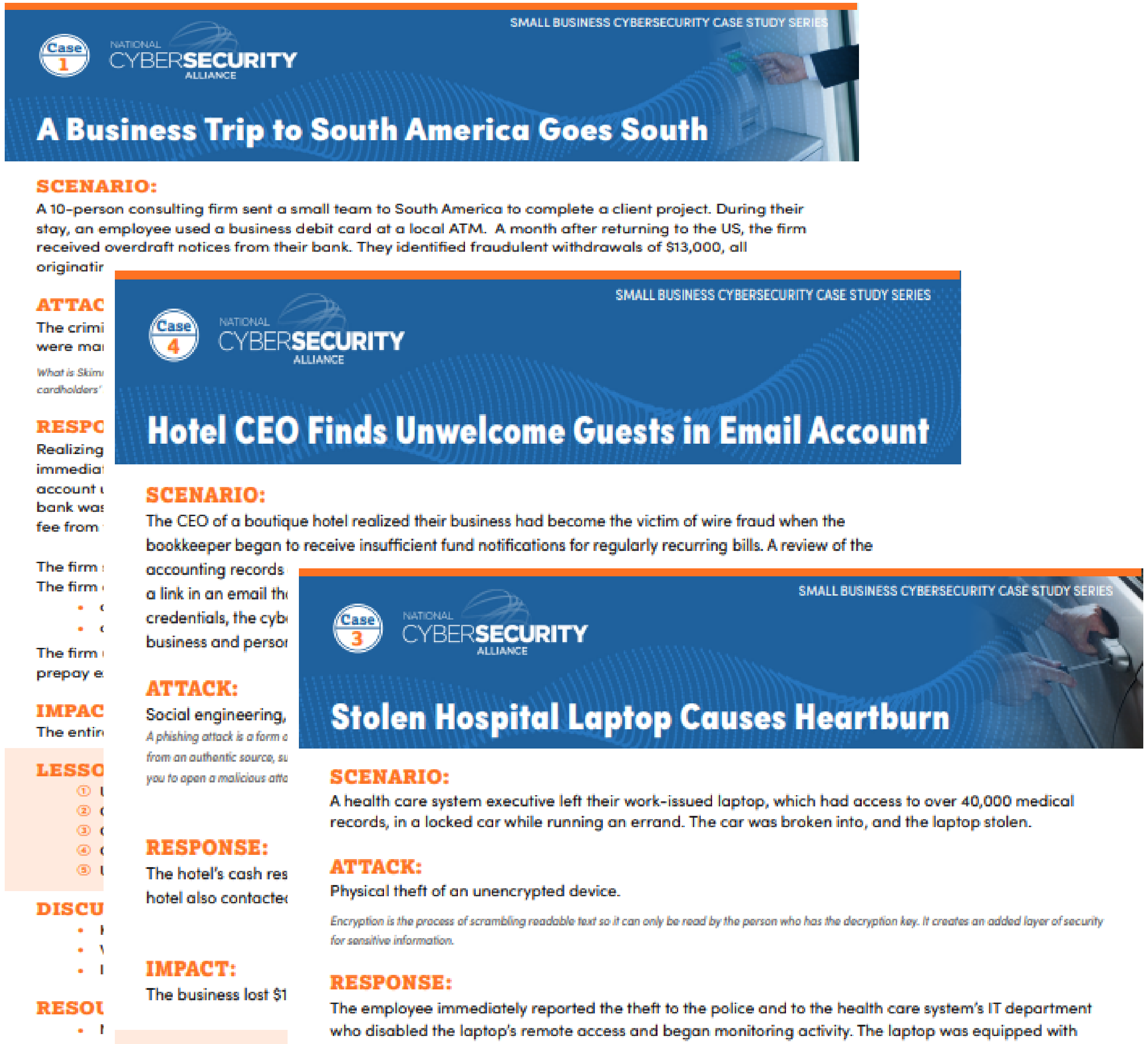


Learn more here.

Short videos that also include a companion PDF handout.

www.nist.gov/itl/smallbusinesscyber/videos

Small Business Case Studies



SMALL BUSINESS CYBERSECURITY CASE STUDY SERIES

Case 1 NATIONAL CYBERSECURITY ALLIANCE

A Business Trip to South America Goes South

SCENARIO:

A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $13,000, all originatir

ATTAC

The crimi were mai

What is Skimi cardholders'

RESPO

Realizing immedia account u bank was fee from

The firm The firm

- c
- c

The firm prepay e

IMPAC

The entir

LESSO

① l
② c
③ c
④ c
⑤ l

DISCU

- I
- V
- I

RESOU

- I

SMALL BUSINESS CYBERSECURITY CASE STUDY SERIES

Case 4 NATIONAL CYBERSECURITY ALLIANCE

Hotel CEO Finds Unwelcome Guests in Email Account

SCENARIO:

The CEO of a boutique hotel realized their business had become the victim of wire fraud when the bookkeeper began to receive insufficient fund notifications for regularly recurring bills. A review of the accounting records a link in an email th credentials, the cyb business and persor

ATTACK:

Social engineering,

A phishing attack is a form o from an authentic source, su you to open a malicious atta

RESPONSE:

The hotel's cash res hotel also contacte

IMPACT:

The business lost $1

SMALL BUSINESS CYBERSECURITY CASE STUDY SERIES

Case 3 NATIONAL CYBERSECURITY ALLIANCE

Stolen Hospital Laptop Causes Heartburn

SCENARIO:

A health care system executive left their work-issued laptop, which had access to over 40,000 medical records, in a locked car while running an errand. The car was broken into, and the laptop stolen.

ATTACK:

Physical theft of an unencrypted device.

Encryption is the process of scrambling readable text so it can only be read by the person who has the decryption key. It creates an added layer of security for sensitive information.

RESPONSE:

The employee immediately reported the theft to the police and to the health care system's IT department who disabled the laptop's remote access and began monitoring activity. The laptop was equipped with

1-page case studies, each including:

- Brief scenario
- Impact to business
- Lessons learned
- Discussion questions
- Related resources

More to come!

nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series

The NIST Small Business Community of Interest (COI)

Over 7,000 individuals have already joined the full COI!

Convening companies, trade associations, and others who can share business insights, expertise, challenges, and perspectives to guide our work and assist NIST to better meet the cybersecurity needs of small businesses.

Learn More Here: https://www.nist.gov/itl/smallbusinesscyber/get-engaged

Manufacturing Extension Partnership (MEP)

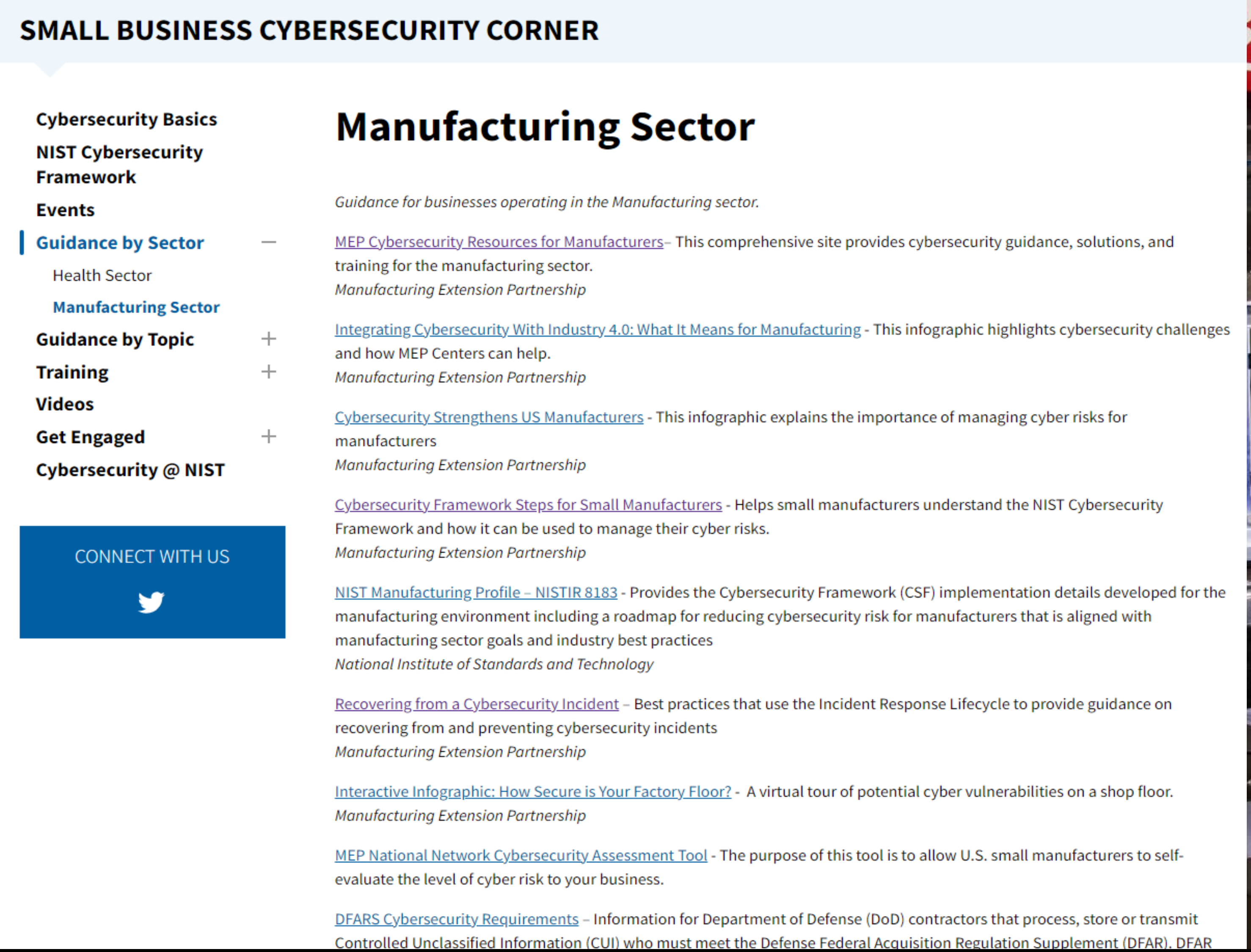
NIST | MANUFACTURING EXTENSION PARTNERSHIP

Providing any U.S. manufacturer with access to resources they need to succeed.

https://www.nist.gov/mep

© Earl Zubkoff

Additional Manufacturing Resources



SMALL BUSINESS CYBERSECURITY CORNER

- Cybersecurity Basics
- NIST Cybersecurity Framework
- Events
- Guidance by Sector —
  - Health Sector
  - Manufacturing Sector
- Guidance by Topic +
- Training +
- Videos
- Get Engaged +
- Cybersecurity @ NIST

CONNECT WITH US

Manufacturing Sector

Guidance for businesses operating in the Manufacturing sector.

MEP Cybersecurity Resources for Manufacturers– This comprehensive site provides cybersecurity guidance, solutions, and training for the manufacturing sector.
Manufacturing Extension Partnership

Integrating Cybersecurity With Industry 4.0: What It Means for Manufacturing - This infographic highlights cybersecurity challenges and how MEP Centers can help.
Manufacturing Extension Partnership

Cybersecurity Strengthens US Manufacturers - This infographic explains the importance of managing cyber risks for manufacturers
Manufacturing Extension Partnership

Cybersecurity Framework Steps for Small Manufacturers - Helps small manufacturers understand the NIST Cybersecurity Framework and how it can be used to manage their cyber risks.
Manufacturing Extension Partnership

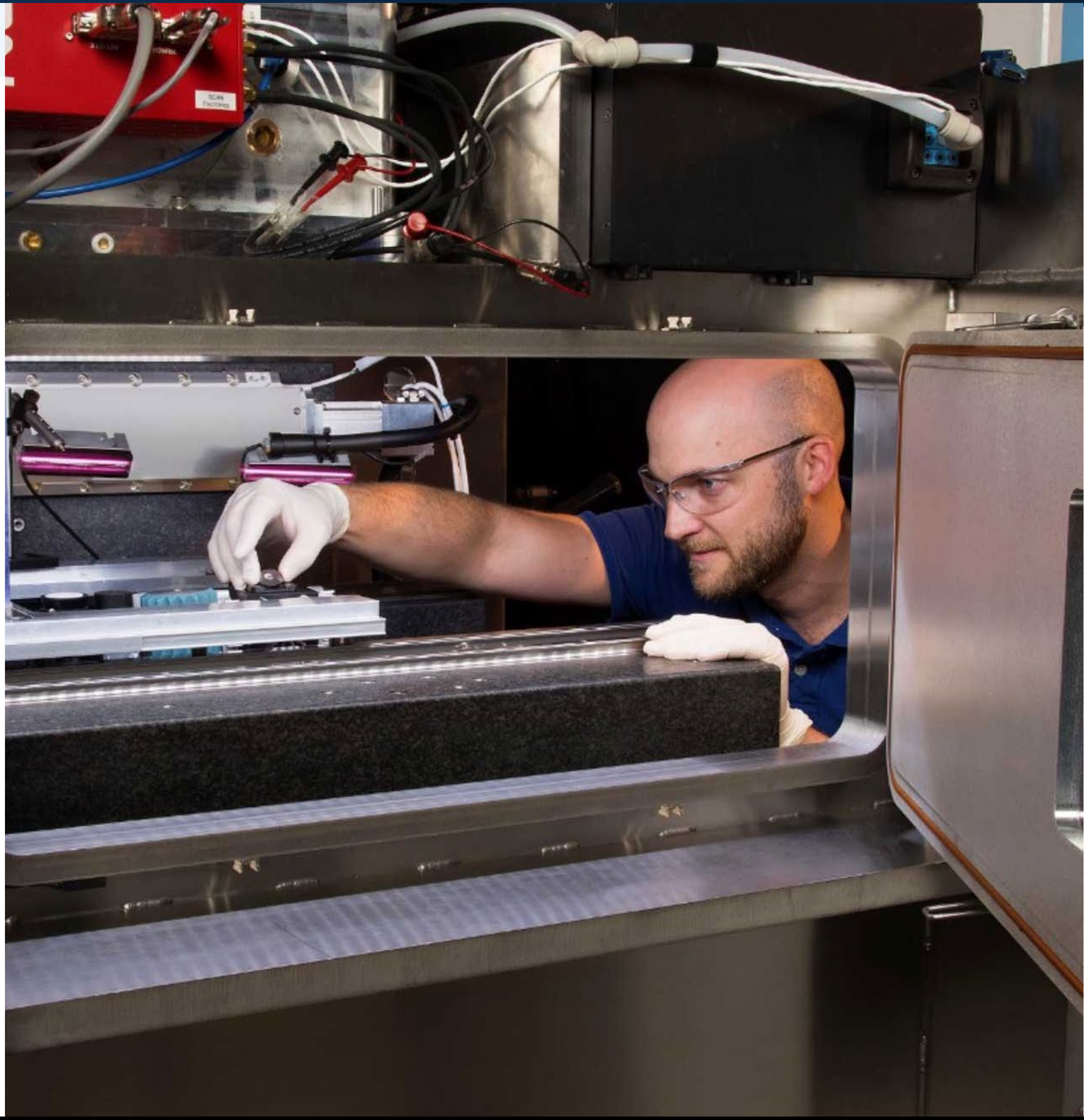
NIST Manufacturing Profile – NISTIR 8183 - Provides the Cybersecurity Framework (CSF) implementation details developed for the manufacturing environment including a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices
National Institute of Standards and Technology

Recovering from a Cybersecurity Incident – Best practices that use the Incident Response Lifecycle to provide guidance on recovering from and preventing cybersecurity incidents
Manufacturing Extension Partnership

Interactive Infographic: How Secure is Your Factory Floor? - A virtual tour of potential cyber vulnerabilities on a shop floor.
Manufacturing Extension Partnership

MEP National Network Cybersecurity Assessment Tool - The purpose of this tool is to allow U.S. small manufacturers to self-evaluate the level of cyber risk to your business.

DFARS Cybersecurity Requirements – Information for Department of Defense (DoD) contractors that process, store or transmit Controlled Unclassified Information (CUI) who must meet the Defense Federal Acquisition Regulation Supplement (DFAR). DFAR



https://www.nist.gov/itl/smallbusinesscyber/health-sector/manufacturing-sector

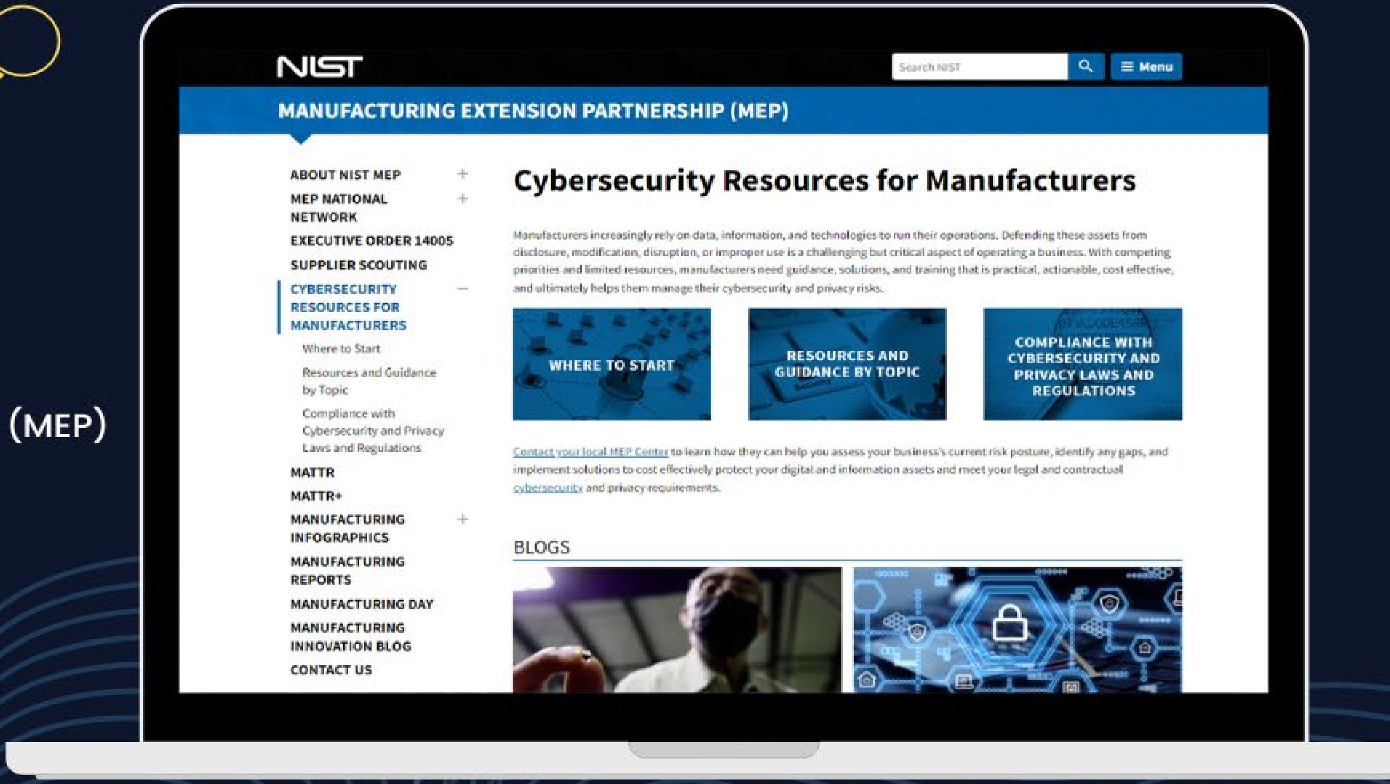
Upcoming Webinar

Cybersecurity Resources for Small to Medium-Sized Manufacturers

A Fireside Chat with the NIST Manufacturing Extension Partnership (MEP)

May 2, 2024

2:00 PM -2:45 PM ET



MANUFACTURING EXTENSION PARTNERSHIP (MEP)

- ABOUT NIST MEP
- MEP NATIONAL NETWORK
- EXECUTIVE ORDER 14005
- SUPPLIER SCOUTING
- CYBERSECURITY RESOURCES FOR MANUFACTURERS
  - Where to Start
  - Resources and Guidance by Topic
  - Compliance with Cybersecurity and Privacy Laws and Regulations
- MATTR
- MATTR+
- MANUFACTURING INFOGRAPHICS
- MANUFACTURING REPORTS
- MANUFACTURING DAY
- MANUFACTURING INNOVATION BLOG
- CONTACT US

Cybersecurity Resources for Manufacturers

Manufacturers increasingly rely on data, information, and technologies to run their operations. Defending these assets from disclosure, modification, disruption, or improper use is a challenging but critical aspect of operating a business. With competing priorities and limited resources, manufacturers need guidance, solutions, and training that is practical, actionable, cost effective, and ultimately helps them manage their cybersecurity and privacy risks.

WHERE TO START

RESOURCES AND GUIDANCE BY TOPIC

COMPLIANCE WITH CYBERSECURITY AND PRIVACY LAWS AND REGULATIONS

Contact your local MEP Center to learn how they can help you assess your business's current risk posture, identify any gaps, and implement solutions to cost effectively protect your digital and information assets and meet your legal and contractual cybersecurity and privacy requirements.

BLOGS

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

https://www.nist.gov/itl/smallbusinesscyber/events

NIST SBIR Program

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

AMERICA'S SEED FUND SBIR·STTR | POWERED BY SBA U.S. Small Business Administration

SBIR Program goals:

1. To increase private sector commercialization of innovations derived from federal R&D;
2. To use small business to meet federal research and development (R&D) needs;
3. To stimulate small business innovation in technology; and
4. To foster and encourage participation by minority and disadvantaged persons in technological innovation.

- NIST's SBIR program is grant-based, and awards are cooperative agreements.
- NIST issues an annual Notice of Funding Opportunity (NOFO) for SBIR Phase I proposals.
- Science and technology-based firms with strong research capabilities in any of the areas listed in the NOFO are encouraged to participate.
- Phase II awards are limited to small businesses that have successfully completed Phase I projects.

https://www.nist.gov/tpo/small-business-innovation-research-program-sbir

Engage with NIST

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Attend our events: https://www.nist.gov/itl/smallbusinesscyber/events

Become an active participant in one of our COI sub-groups: https://www.nist.gov/itl/smallbusinesscyber/about-contact-us/subscribe

Send questions, comments, project ideas or request a speaker for your event: smallbizsecurity@nist.gov

Submit comments on our publications: csrc.nist.gov/publications/drafts-open-for-comment

Become a collaborator on an NCCoE project: https://www.nccoe.nist.gov/seeking-collaborators

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Questions?

https://www.nist.gov/itl/smallbusinesscyber

smallbizsecurity@nist.gov

AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza

DAF CISO's
Blue Cyber Initiative

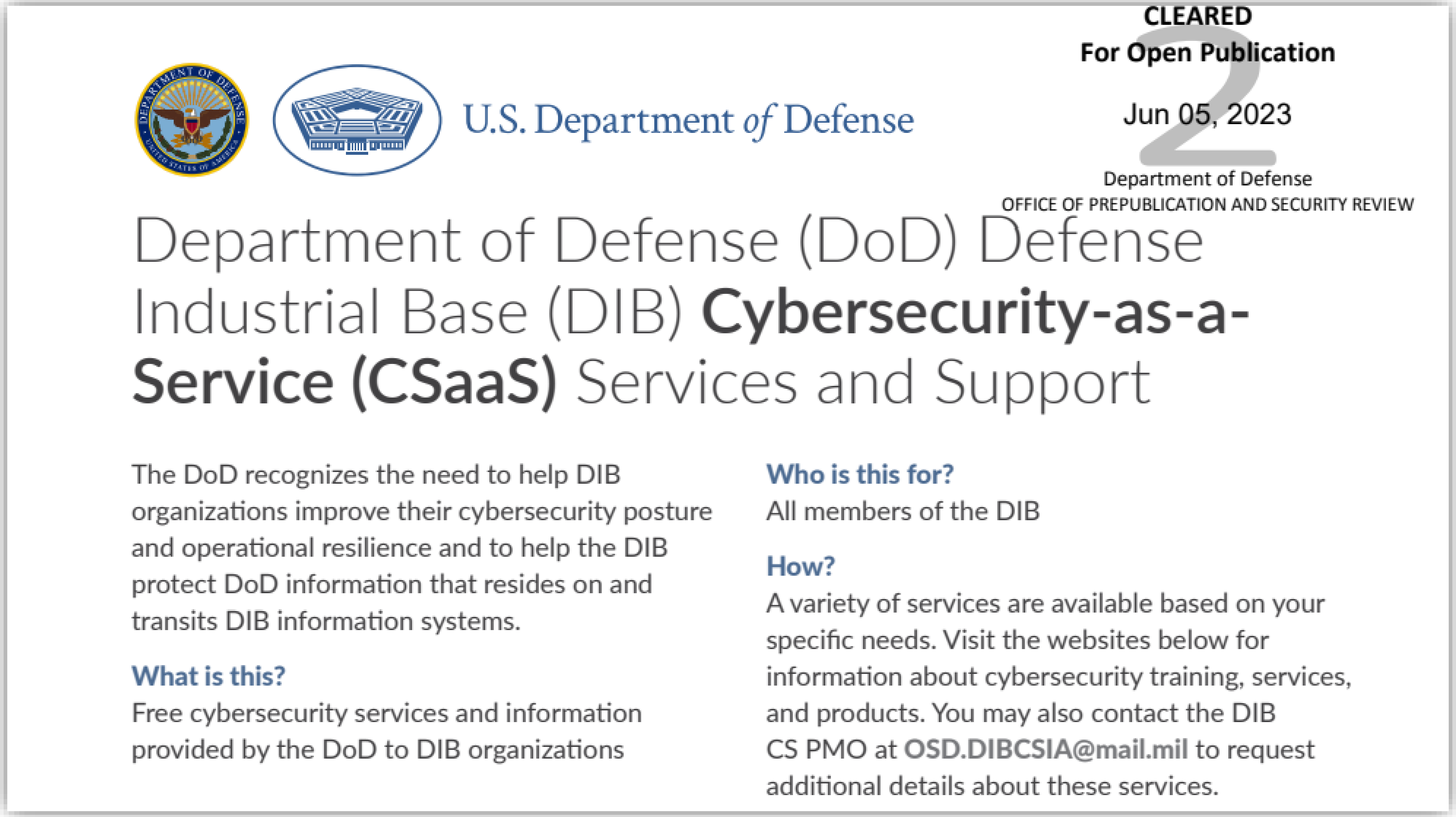
Kelley Kiernan

AFWERX

Jan 30, 2024

BLUE CYBER EDUCATION SERIES

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.



CLEARED
For Open Publication

Jun 05, 2023

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

U.S. Department *of* Defense

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

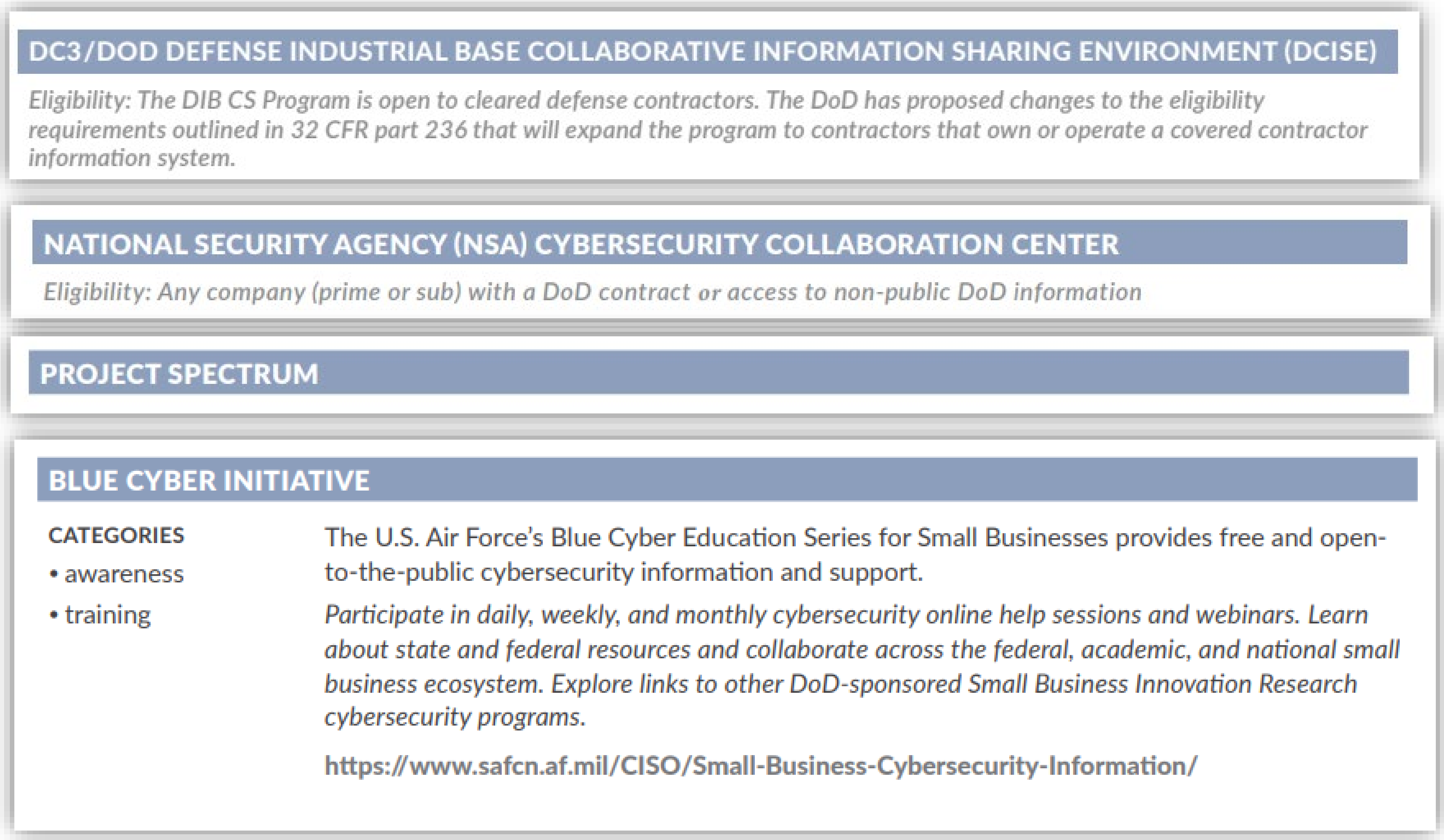
Who is this for?

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.

DAF CISO’S BLUE CYBER



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.

NATIONAL SECURITY AGENCY (NSA) CYBERSECURITY COLLABORATION CENTER

Eligibility: Any company (prime or sub) with a DoD contract or access to non-public DoD information

PROJECT SPECTRUM

BLUE CYBER INITIATIVE

CATEGORIES

- awareness
- training

The U.S. Air Force’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/

file:///C:/Users/1139598403C/OneDrive%20-%20United%20States%20Air%20Force/Documents/00%20Events/Flyers/DOD%20CIO%20DIB%20Cybersecurity%20Services%20Sheet_CSaaS%20v1.0.pdf

DAILY, Open Office Hours

Daily
Event

DAILY OFFICE HOURS

- Register here: www.safcn.af.mil/CISO/small-business-cybersecurity-information/
- Nearly-daily opportunity to ask questions and get answers in-person.
- More information at https://www.safcn.af.mil/Contact-Us/

EVERY-TUESDAY, Small Business Cybersecurity ASK-ME-ANYTHING

Weekly Event

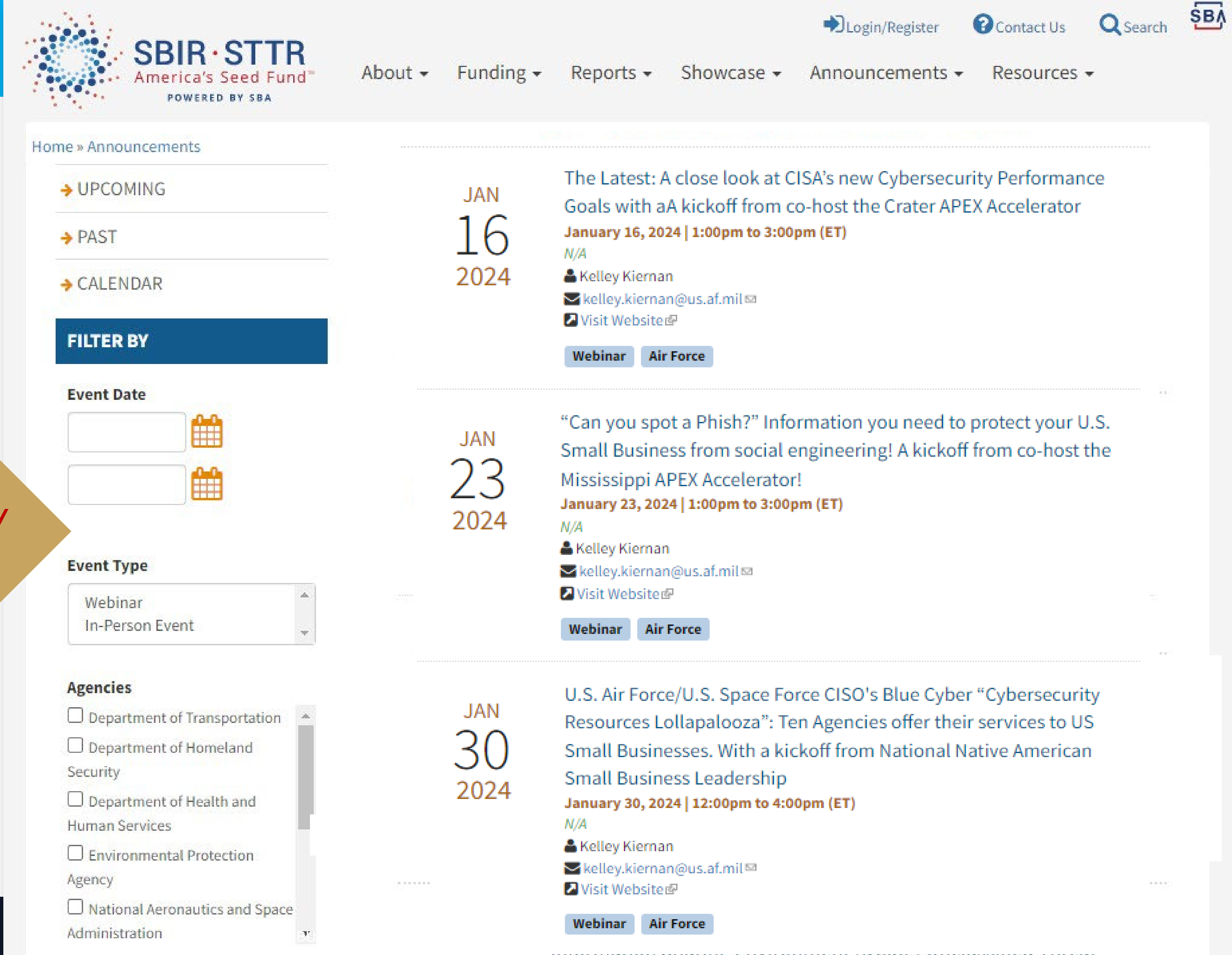
Weekly Event

WEEKLY – Every Tuesday 1pm Eastern

- Register here: www.sbir.gov/events
- A guest speaker will cover an ultra-relevant small business cybersecurity topic and get your cybersecurity/information protection questions answered.
- More information from https://www.safcn.af.mil/Contact-Us/

All our Events

www.sbir.gov/events



Home » Announcements

- UPCOMING
- PAST
- CALENDAR

FILTER BY

Event Date

Event Type

Webinar
In-Person Event

Agencies

□ Department of Transportation
□ Department of Homeland Security
□ Department of Health and Human Services
□ Environmental Protection Agency
□ National Aeronautics and Space Administration

JAN 16 2024

The Latest: A close look at CISA's new Cybersecurity Performance Goals with aA kickoff from co-host the Crater APEX Accelerator

January 16, 2024 | 1:00pm to 3:00pm (ET)

N/A

Kelley Kiernan

kelley.kiernan@us.af.mil

Visit Website

Webinar **Air Force**

JAN 23 2024

"Can you spot a Phish?" Information you need to protect your U.S. Small Business from social engineering! A kickoff from co-host the Mississippi APEX Accelerator!

January 23, 2024 | 1:00pm to 3:00pm (ET)

N/A

Kelley Kiernan

kelley.kiernan@us.af.mil

Visit Website

Webinar **Air Force**

JAN 30 2024

U.S. Air Force/U.S. Space Force CISO's Blue Cyber "Cybersecurity Resources Lollapalooza": Ten Agencies offer their services to US Small Businesses. With a kickoff from National Native American Small Business Leadership

January 30, 2024 | 12:00pm to 4:00pm (ET)

N/A

Kelley Kiernan

kelley.kiernan@us.af.mil

Visit Website

Webinar **Air Force**

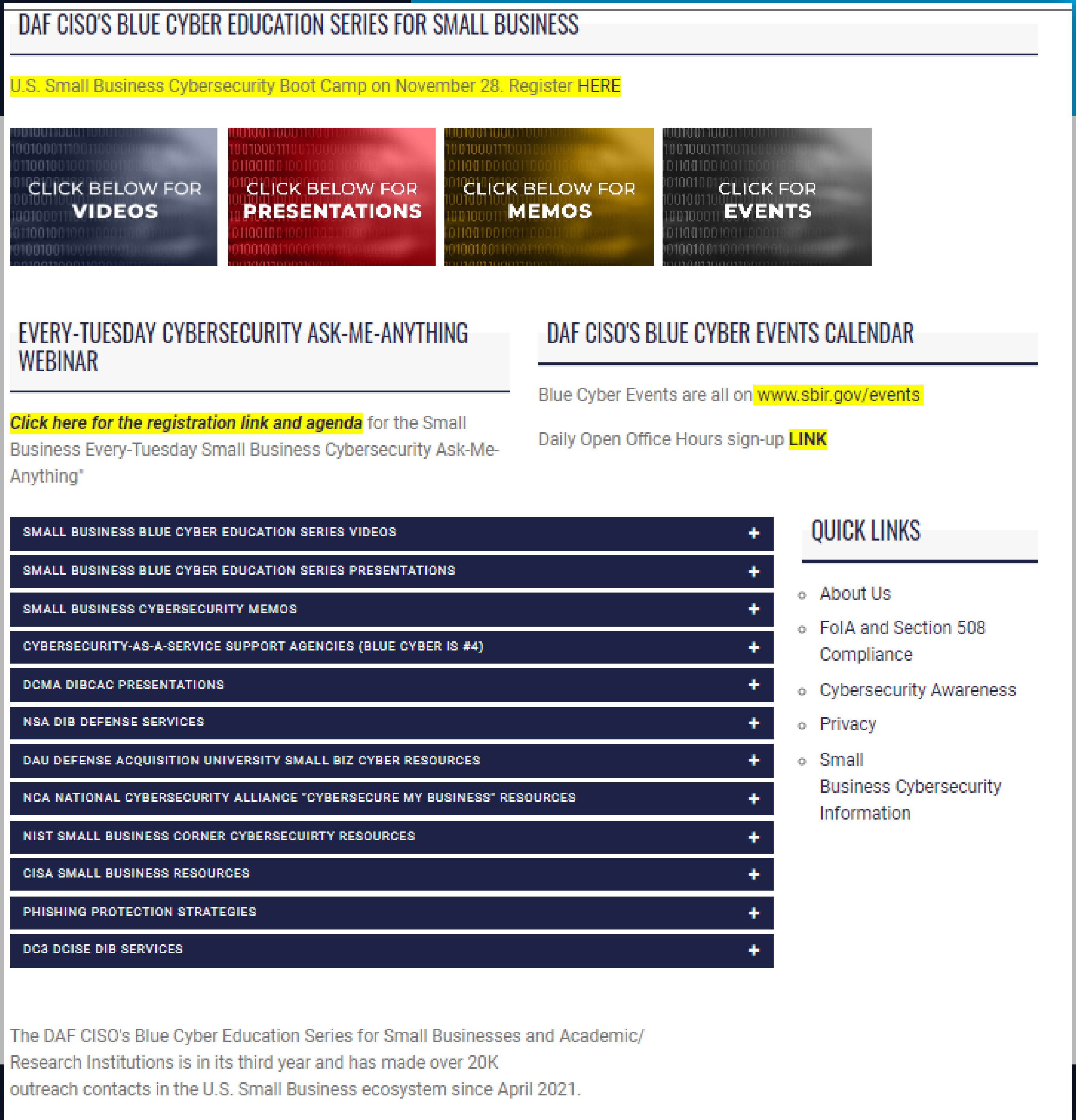
Everybody Handles Federal Contracting Information!

Walk Through of the FAR 52.204-21 and proposed CMMC Level 1

Monthly Event

MONTHLY – TBD February 1pm-3pm EST

- Register here: www.sbir.gov/events
- The Blue Cyber Director, Kelley Kiernan will cover the 15 security requirements in the proposed CMMC Level 1 and FAR 52.204-21, which comprise basic cyber hygiene for your small business.
- More information from https://www.safcn.af.mil/Contact-Us/



DAF CISO'S BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

U.S. Small Business Cybersecurity Boot Camp on November 28. Register HERE

EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING WEBINAR

Click here for the registration link and agenda for the Small Business Every-Tuesday Small Business Cybersecurity Ask-Me-Anything"

DAF CISO'S BLUE CYBER EVENTS CALENDAR

Blue Cyber Events are all on www.sbir.gov/events

Daily Open Office Hours sign-up **LINK**

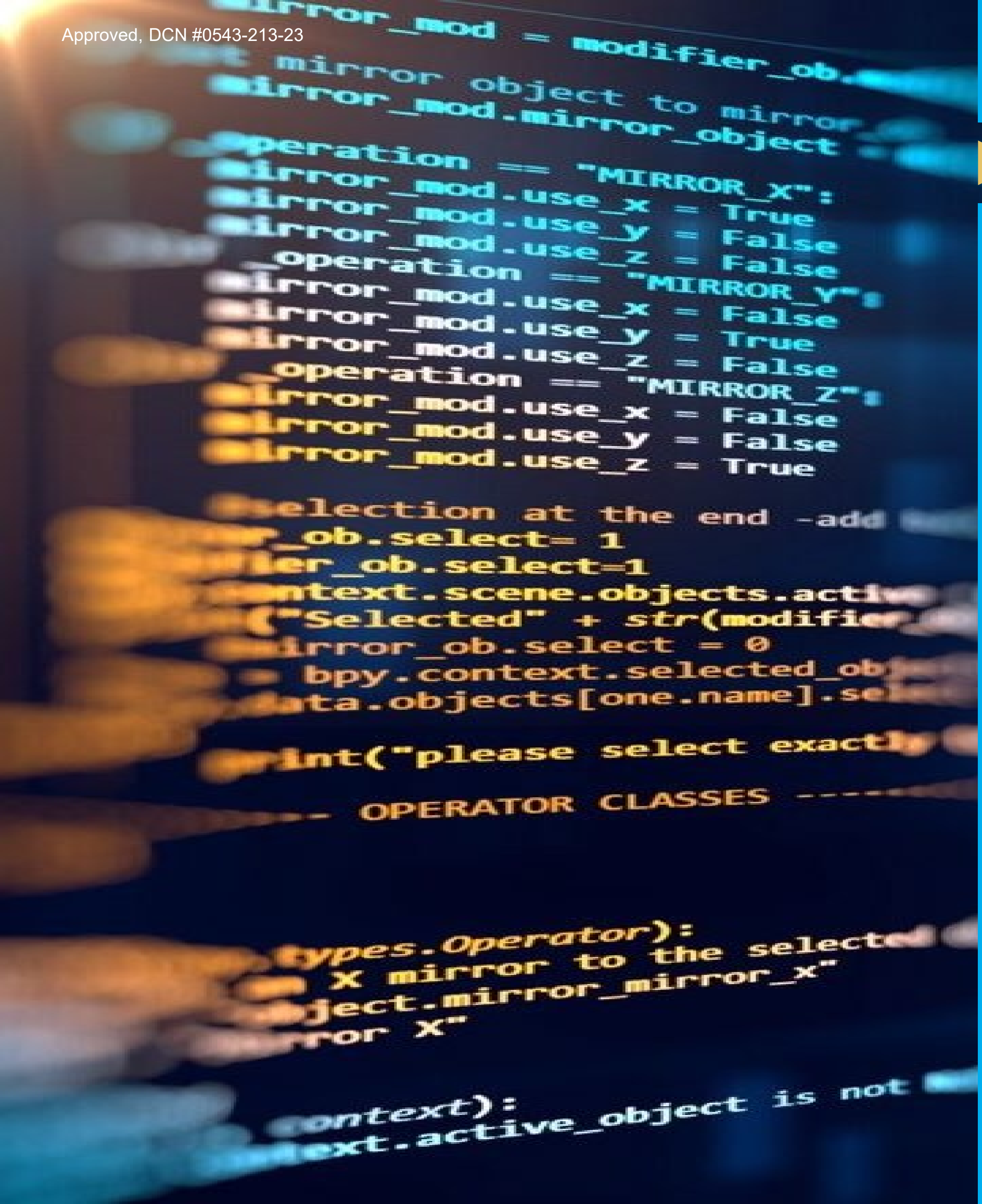
- SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS +
- SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS +
- SMALL BUSINESS CYBERSECURITY MEMOS +
- CYBERSECURITY-AS-A-SERVICE SUPPORT AGENCIES (BLUE CYBER IS #4) +
- DCMA DIBCAC PRESENTATIONS +
- NSA DIB DEFENSE SERVICES +
- DAU DEFENSE ACQUISITION UNIVERSITY SMALL BIZ CYBER RESOURCES +
- NCA NATIONAL CYBERSECURITY ALLIANCE "CYBERSECURE MY BUSINESS" RESOURCES +
- NIST SMALL BUSINESS CORNER CYBERSECUIRTY RESOURCES +
- CISA SMALL BUSINESS RESOURCES +
- PHISHING PROTECTION STRATEGIES +
- DC3 DCISE DIB SERVICES +

QUICK LINKS

- About Us
- FoIA and Section 508 Compliance
- Cybersecurity Awareness
- Privacy
- Small Business Cybersecurity Information

The DAF CISO's Blue Cyber Education Series for Small Businesses and Academic/ Research Institutions is in its third year and has made over 20K outreach contacts in the U.S. Small Business ecosystem since April 2021.

Approved, DCN #0543-213-23

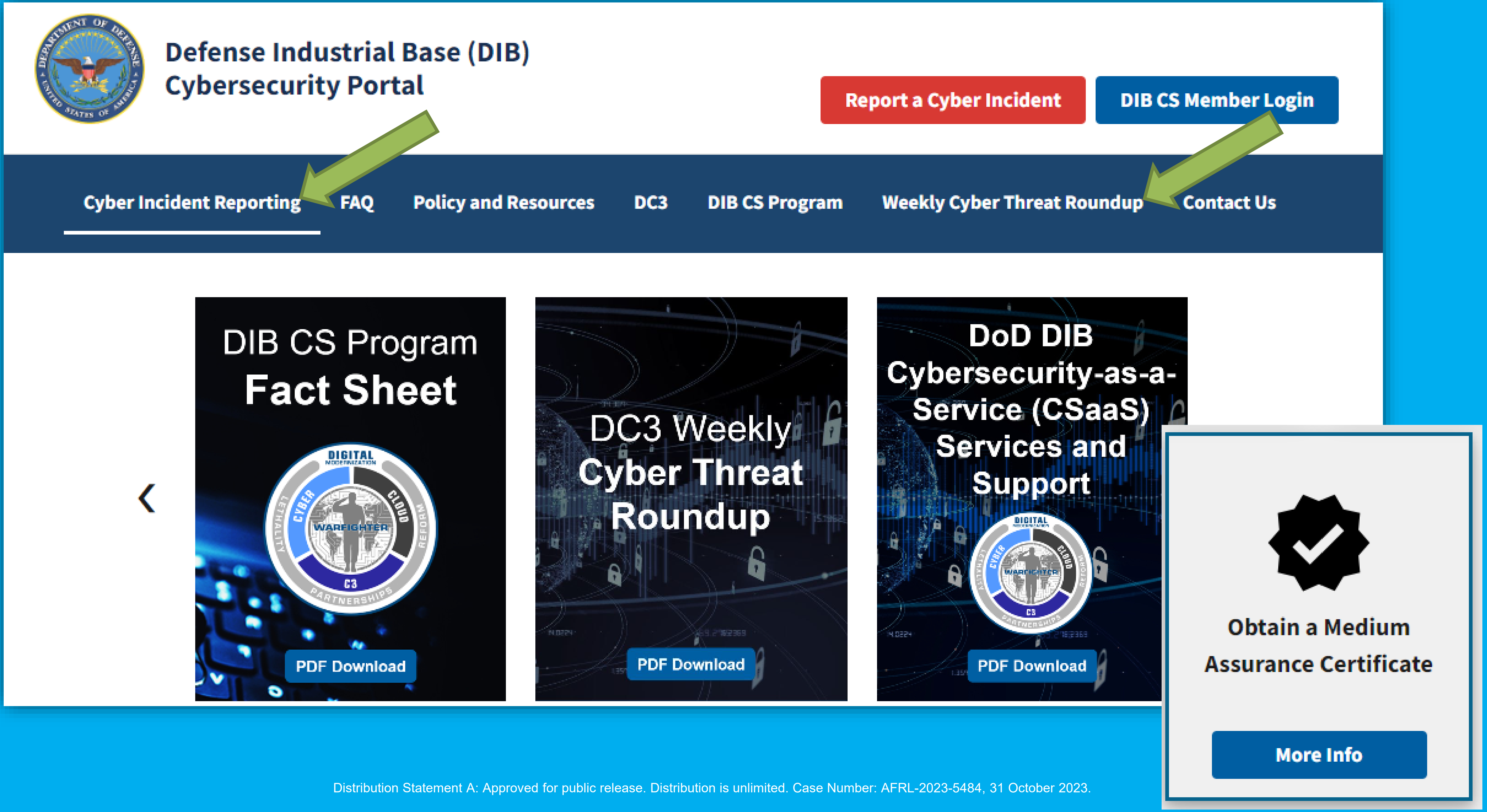


```
irror_mod = modifier_ob
mirror object to mirror
irror_mod.mirror_object
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifie
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactl

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
ror X"

ontext):
ext.active_object is not
```

AN OFFERING IN THE BLUE CYBER SERIES

If you are a DOD contractor, You must report cyber incidents to DC3

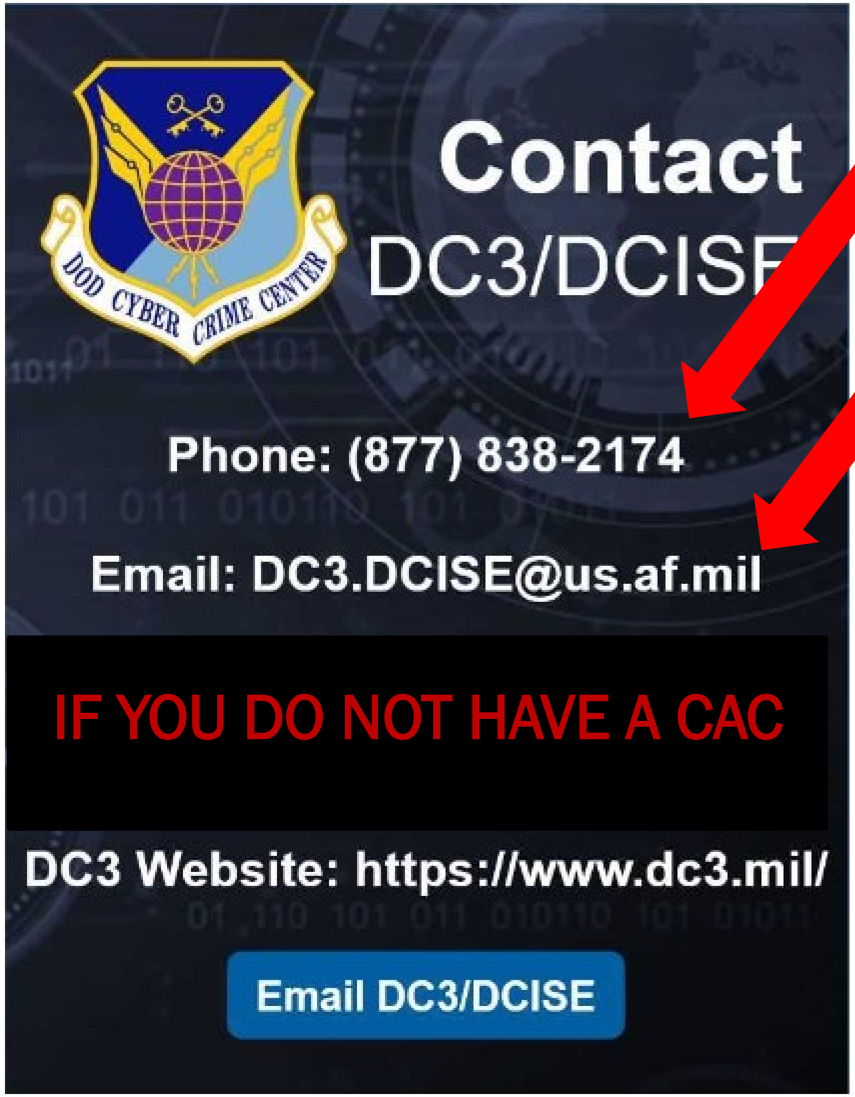
https://dibnet.dod.mil/dibnet/



Defense Industrial Base (DIB) Cybersecurity Portal

Report a Cyber Incident
DIB CS Member Login
Cyber Incident Reporting
FAQ
Policy and Resources
DC3
DIB CS Program
Weekly Cyber Threat Roundup
Contact Us
DIB CS Program Fact Sheet
PDF Download
DC3 Weekly Cyber Threat Roundup
PDF Download
DoD DIB Cybersecurity-as-a-Service (CSaaS) Services and Support
PDF Download
Obtain a Medium Assurance Certificate
More Info

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.



Contact DC3/DCISE

Phone: (877) 838-2174

Email: DC3.DCISE@us.af.mil

IF YOU DO NOT HAVE A CAC

DC3 Website: https://www.dc3.mil/

A DoD-Approved Medium Assurance Certificate is required to report a cyber incident via the portal.

If you do not have a DoD-approved Medium Assurance Certificate

- please email DC3.DCISE@us.af.mil or
- call the DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE) hotline at (410) 981-0104 for further assistance.

This information repeats under the FAQs on the page

Internet Crime Complaint Center (IC3)

www.ic3.gov

Protect one another.

The Internet Crime Complaint Center, or IC3, is the Nation's central hub for reporting cyber crime. It is run by the FBI, the lead federal agency for investigating cyber crime. Here on our website, you can take two vital steps to protecting cyberspace and your own online security.

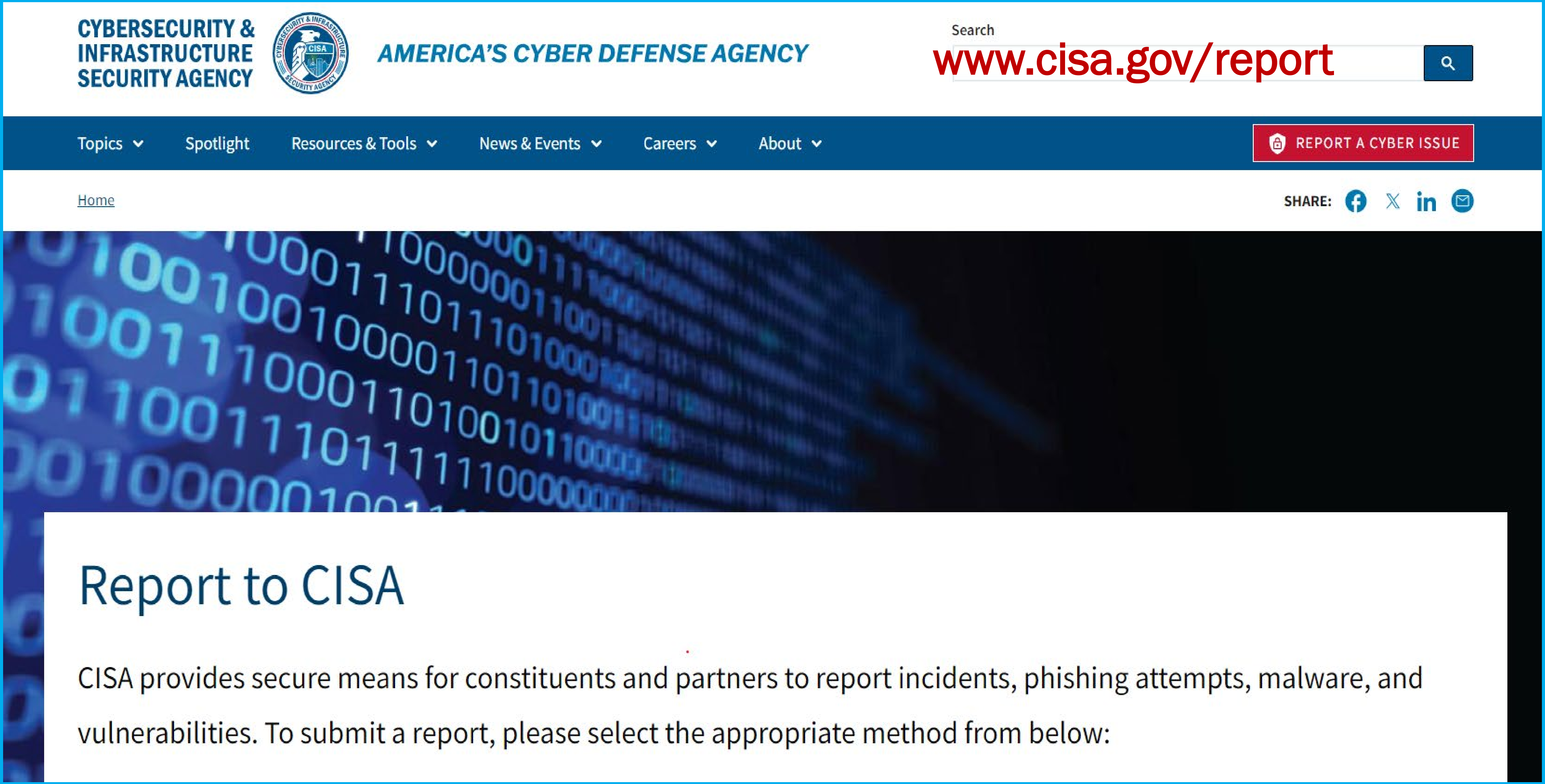
First, if you believe you have fallen victim to cyber crime, file a complaint or report. Your information is invaluable to helping the FBI and its partners bring cybercriminals to justice.

Second, get educated about the latest and most harmful cyber threats and scams. By doing so, you will be better able to protect yourself, your family, and your place of work.

Anyone can become a victim of internet crime. Take action for yourself and others by reporting it. Reporting internet crimes can help bring criminals to justice and make the internet a safer place for us all.

File a Complaint

Join the fight against internet crime!



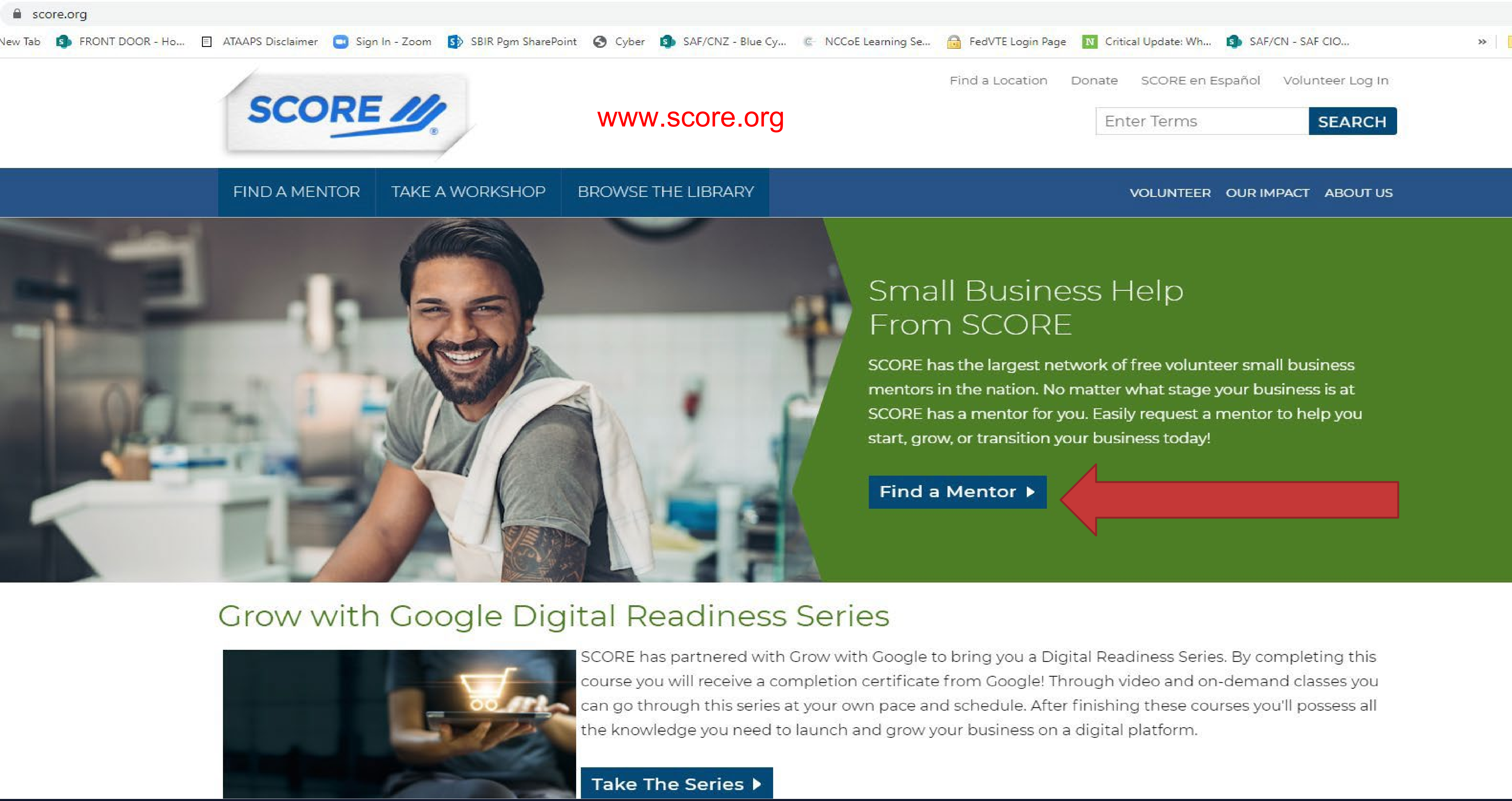
www.cisa.gov/report

Report to CISA

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To submit a report, please select the appropriate method from below:

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

www.score.org



Small Business Help From SCORE

SCORE has the largest network of free volunteer small business mentors in the nation. No matter what stage your business is at SCORE has a mentor for you. Easily request a mentor to help you start, grow, or transition your business today!

Grow with Google Digital Readiness Series

SCORE has partnered with Grow with Google to bring you a Digital Readiness Series. By completing this course you will receive a completion certificate from Google! Through video and on-demand classes you can go through this series at your own pace and schedule. After finishing these courses you'll possess all the knowledge you need to launch and grow your business on a digital platform.

FCC CYBER PLANNING GUIDE

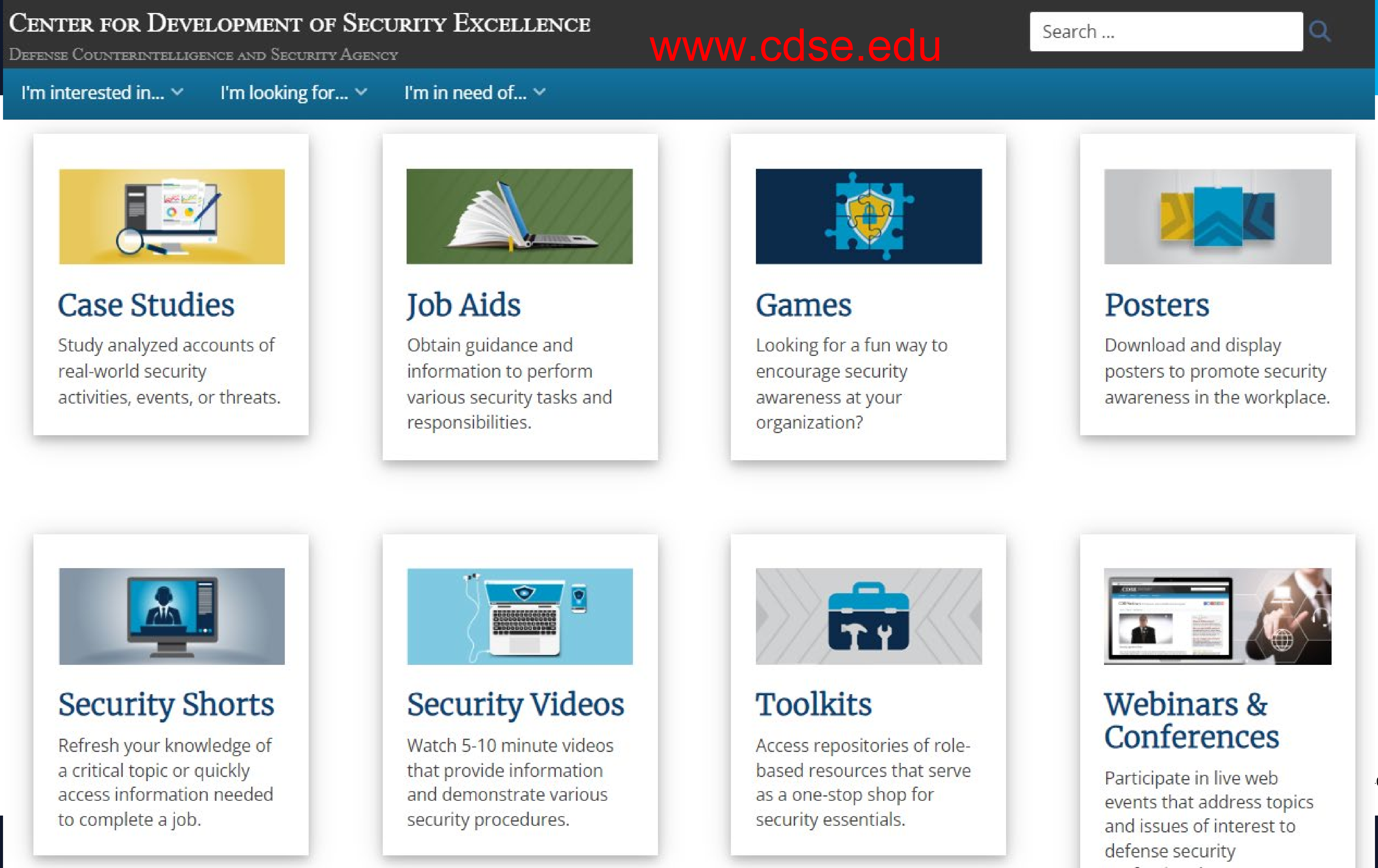
www.fcc.gov/cyberplanner

- Privacy and Data Security
- Scams and Fraud
- Network Security
- Website Security
- Email
- Mobile Devices
- Employees
- Facility Security
- Operational Security
- Payment Cards
- Incident Response and Reporting
- Policy Development, Management

Federal Communications Commission

Cyber Security Planning Guide

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.



www.cdse.edu

Center for Development of Security Excellence

Defense Counterintelligence and Security Agency

Case Studies

Study analyzed accounts of real-world security activities, events, or threats.

Job Aids

Obtain guidance and information to perform various security tasks and responsibilities.

Games

Looking for a fun way to encourage security awareness at your organization?

Posters

Download and display posters to promote security awareness in the workplace.

Security Shorts

Refresh your knowledge of a critical topic or quickly access information needed to complete a job.

Security Videos

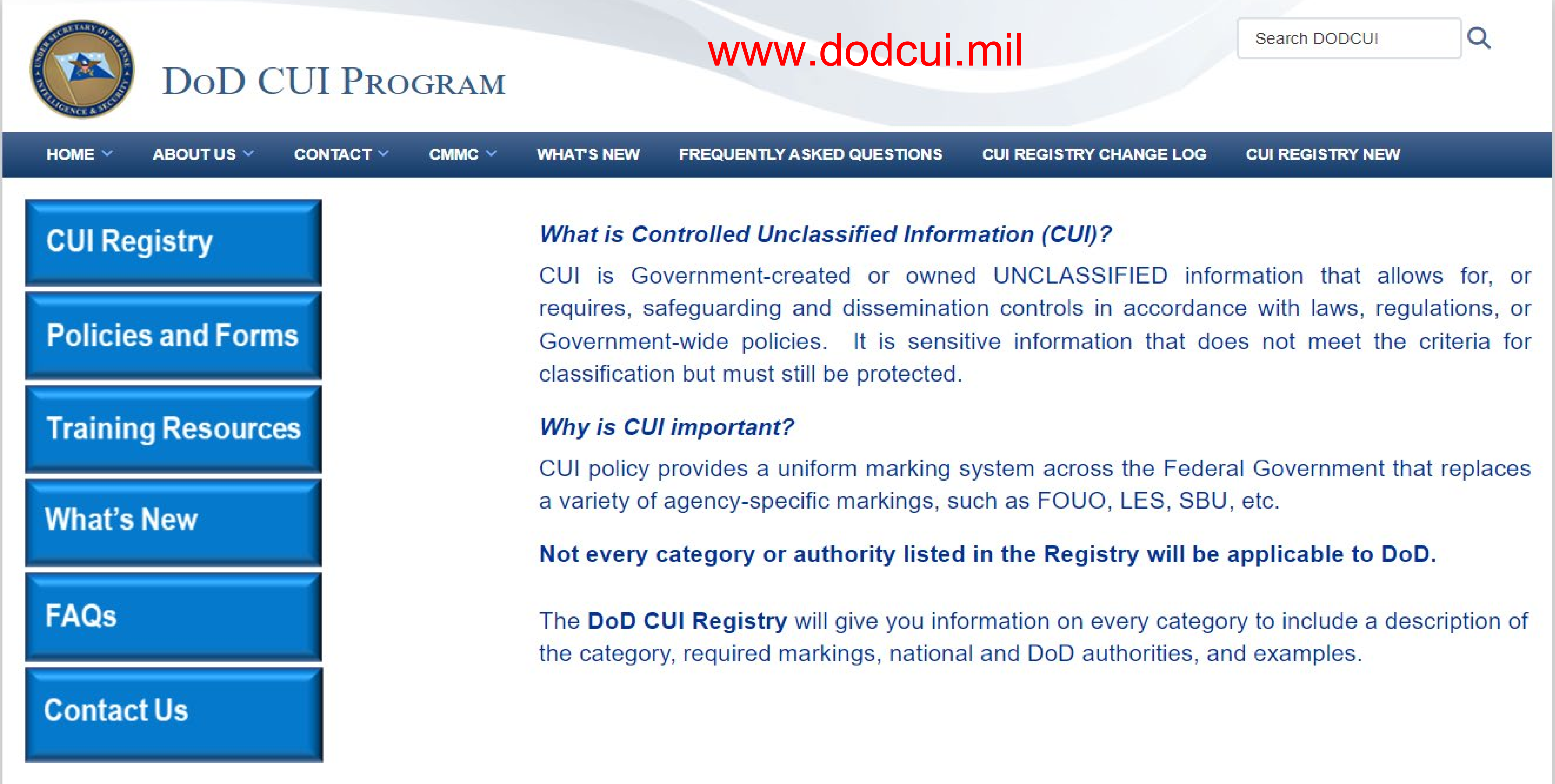
Watch 5-10 minute videos that provide information and demonstrate various security procedures.

Toolkits

Access repositories of role-based resources that serve as a one-stop shop for security essentials.

Webinars & Conferences

Participate in live web events that address topics and issues of interest to defense security www.dodcui.mil



What is Controlled Unclassified Information (CUI)?

CUI is Government-created or owned UNCLASSIFIED information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies. It is sensitive information that does not meet the criteria for classification but must still be protected.

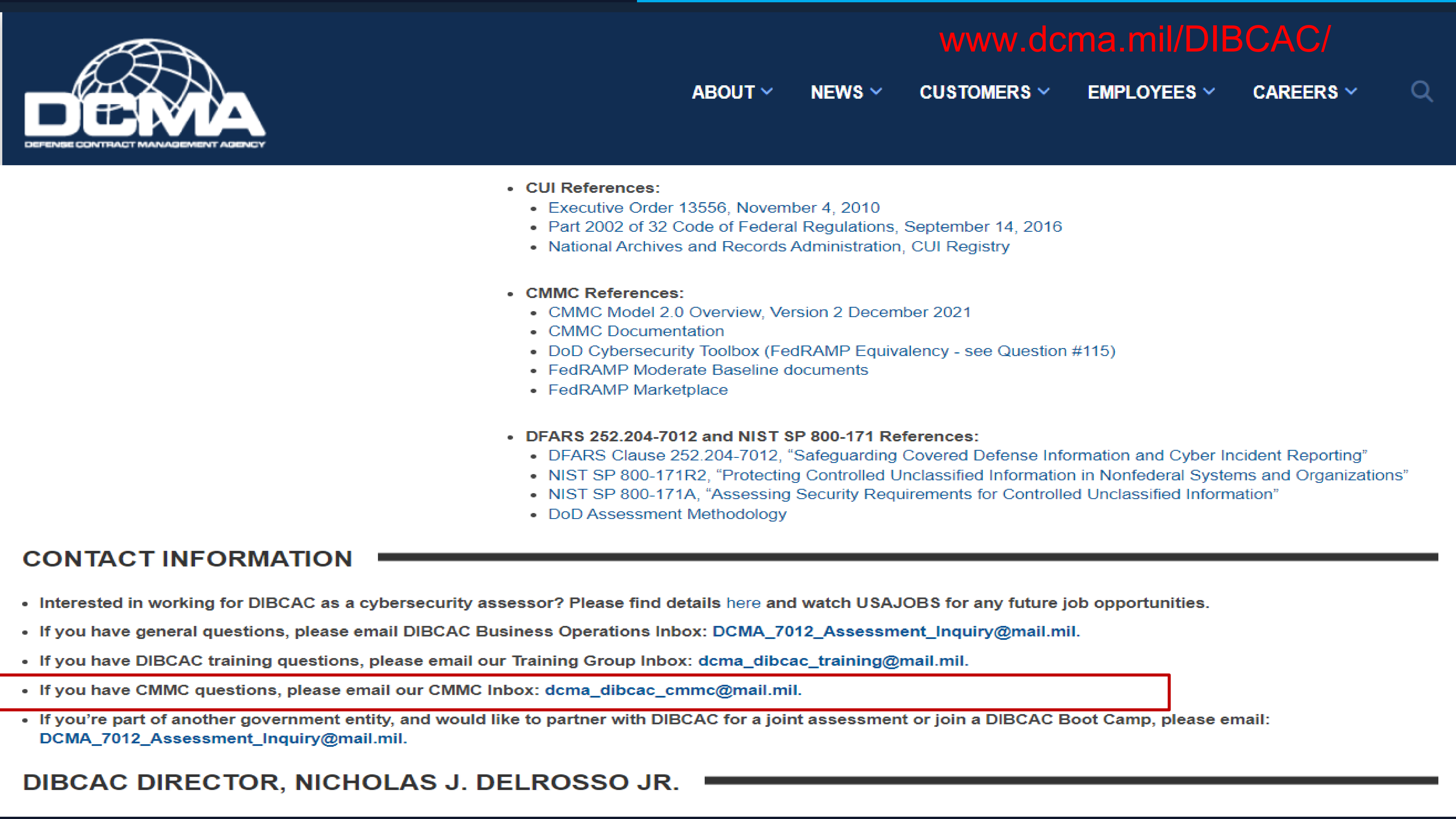
Why is CUI important?

CUI policy provides a uniform marking system across the Federal Government that replaces a variety of agency-specific markings, such as FOUO, LES, SBU, etc.

Not every category or authority listed in the Registry will be applicable to DoD.

The **DoD CUI Registry** will give you information on every category to include a description of the category, required markings, national and DoD authorities, and examples.

www.dcma.mil/DIBCAC/



- **CUI References:**
  - Executive Order 13556, November 4, 2010
  - Part 2002 of 32 Code of Federal Regulations, September 14, 2016
  - National Archives and Records Administration, CUI Registry

- **CMMC References:**
  - CMMC Model 2.0 Overview, Version 2 December 2021
  - CMMC Documentation
  - DoD Cybersecurity Toolbox (FedRAMP Equivalency - see Question #115)
  - FedRAMP Moderate Baseline documents
  - FedRAMP Marketplace

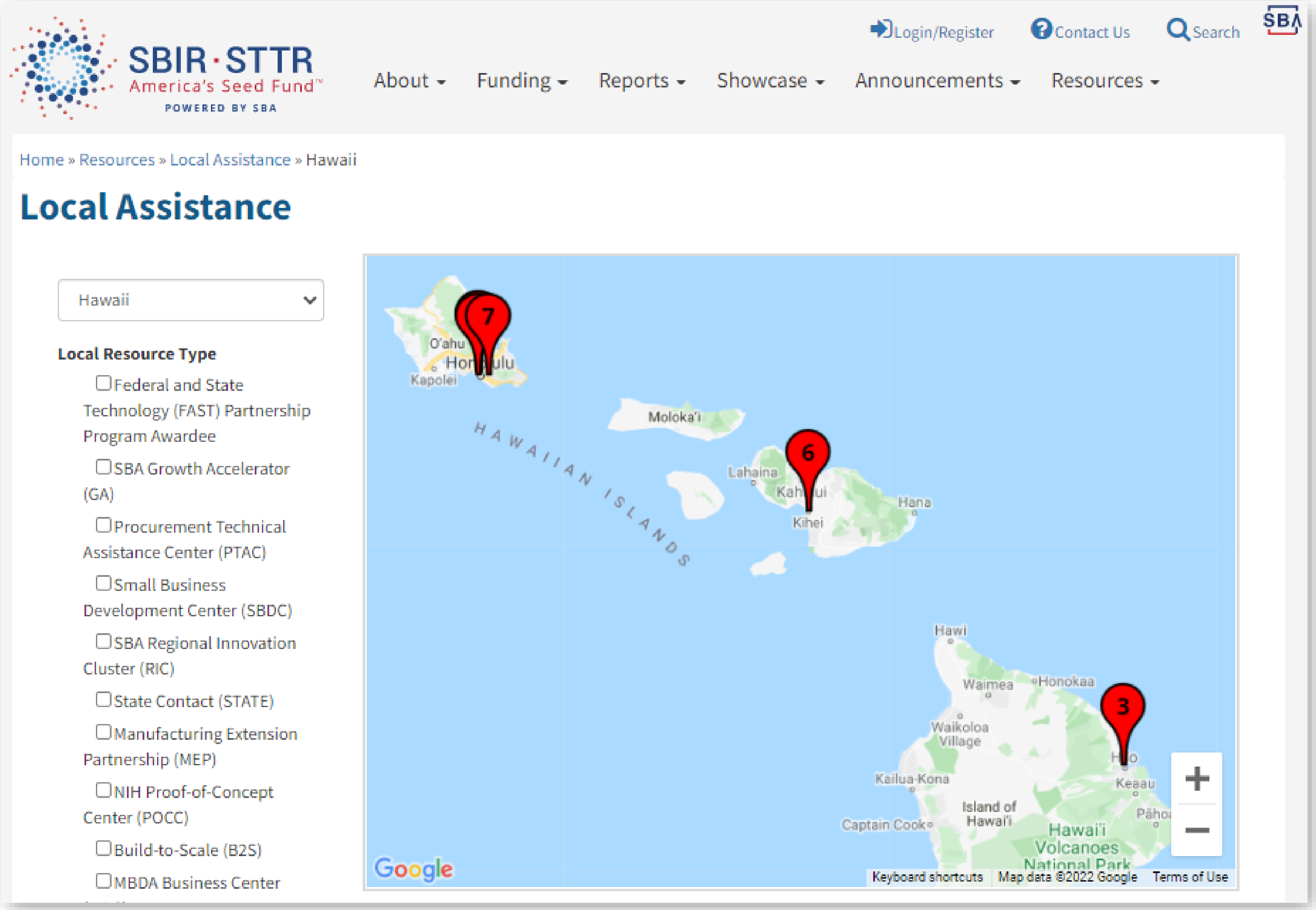
- **DFARS 252.204-7012 and NIST SP 800-171 References:**
  - DFARS Clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”
  - NIST SP 800-171R2, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”
  - NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information”
  - DoD Assessment Methodology

CONTACT INFORMATION

- **Interested in working for DIBCAC as a cybersecurity assessor? Please find details here and watch USAJOBS for any future job opportunities.**
- **If you have general questions, please email DIBCAC Business Operations Inbox: DCMA_7012_Assessment_Inquiry@mail.mil.**
- **If you have DIBCAC training questions, please email our Training Group Inbox: dcma_dibcac_training@mail.mil.**
- **If you have CMMC questions, please email our CMMC Inbox: dcma_dibcac_cmmc@mail.mil.**
- **If you’re part of another government entity, and would like to partner with DIBCAC for a joint assessment or join a DIBCAC Boot Camp, please email: DCMA_7012_Assessment_Inquiry@mail.mil.**

DIBCAC DIRECTOR, NICHOLAS J. DELROSSO JR.

DAF CISO'S BLUE CYBER



Home » Resources » Local Assistance » Hawaii

Local Assistance

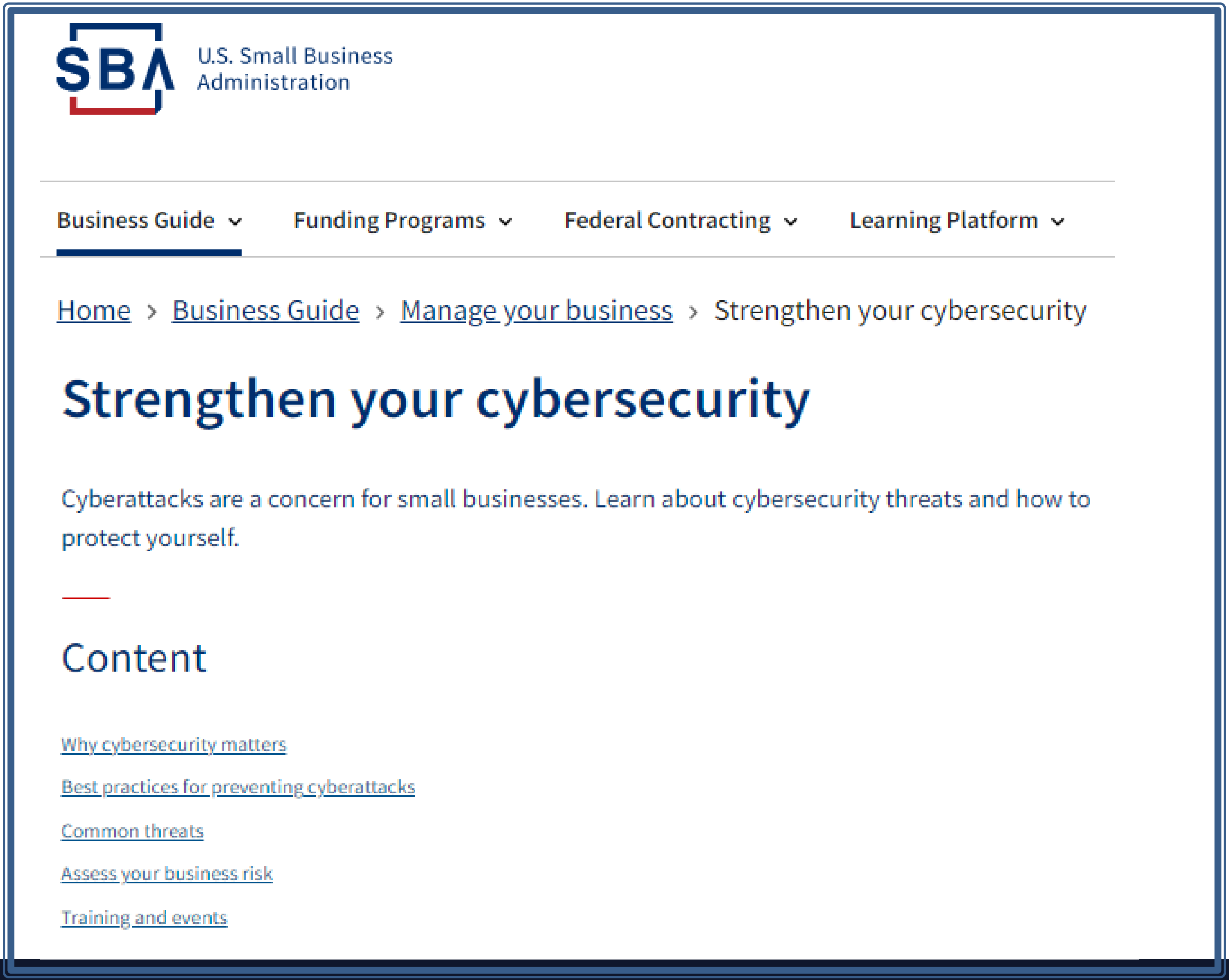
Hawaii

Local Resource Type

- ☐ Federal and State Technology (FAST) Partnership Program Awardee
- ☐ SBA Growth Accelerator (GA)
- ☐ Procurement Technical Assistance Center (PTAC)
- ☐ Small Business Development Center (SBDC)
- ☐ SBA Regional Innovation Cluster (RIC)
- ☐ State Contact (STATE)
- ☐ Manufacturing Extension Partnership (MEP)
- ☐ NIH Proof-of-Concept Center (POCC)
- ☐ Build-to-Scale (B2S)
- ☐ MBDA Business Center

www.sbir.gov/local-assistance

DAF CISO'S BLUE CYBER



Home > Business Guide > Manage your business > Strengthen your cybersecurity

Strengthen your cybersecurity

Cyberattacks are a concern for small businesses. Learn about cybersecurity threats and how to protect yourself.

Content

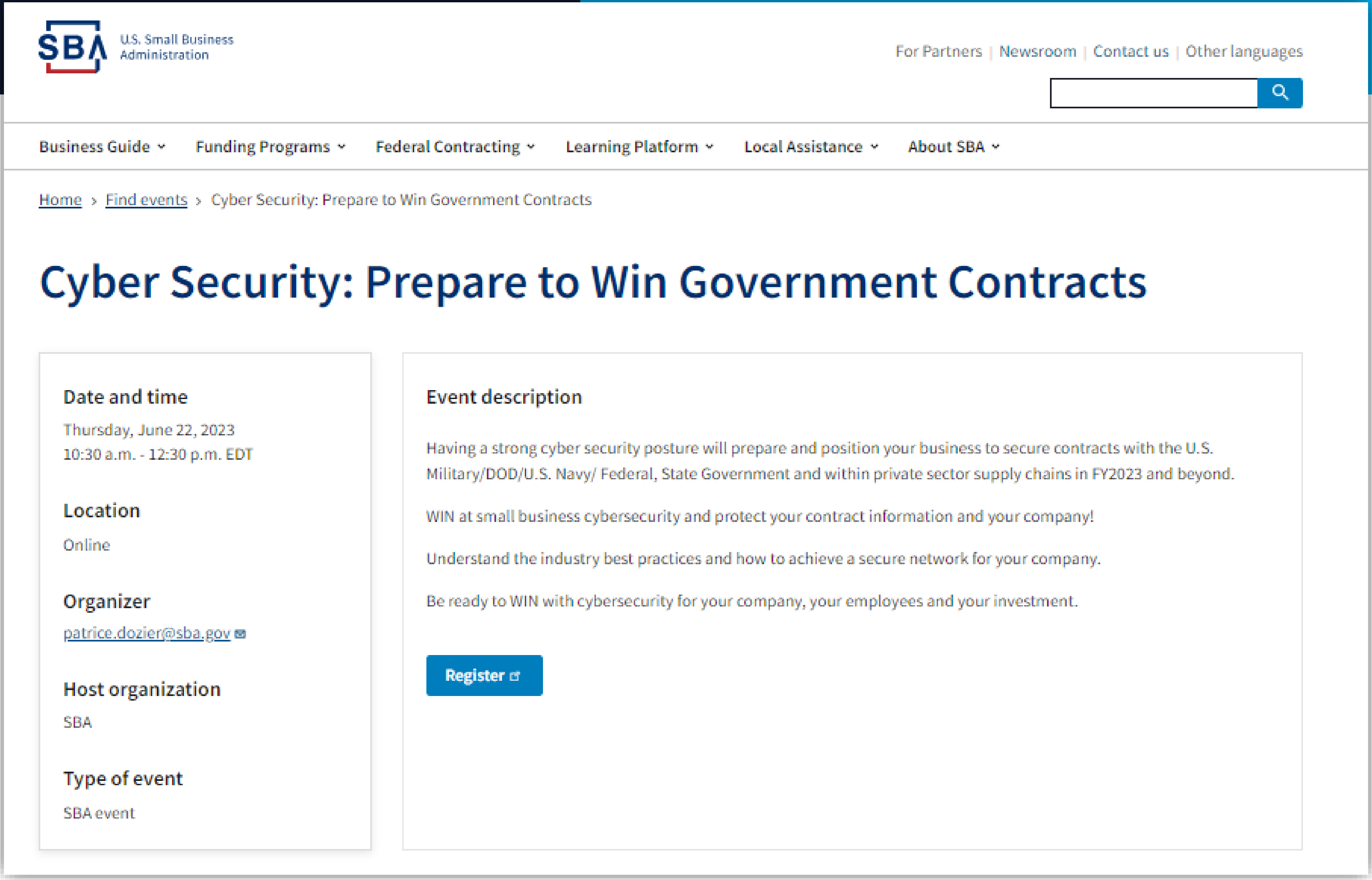
Why cybersecurity matters

Best practices for preventing cyberattacks

Common threats

Assess your business risk

Training and events


U.S. Small Business Administration
For Partners | Newsroom | Contact us | Other languages
Business Guide
Funding Programs
Federal Contracting
Learning Platform
Local Assistance
About SBA
Home › Find events › Cyber Security: Prepare to Win Government Contracts
Register

Cyber Security: Prepare to Win Government Contracts

Date and time

Thursday, June 22, 2023
10:30 a.m. - 12:30 p.m. EDT

Location

Online

Organizer

patrice.dozier@sba.gov

Host organization

SBA

Type of event

SBA event

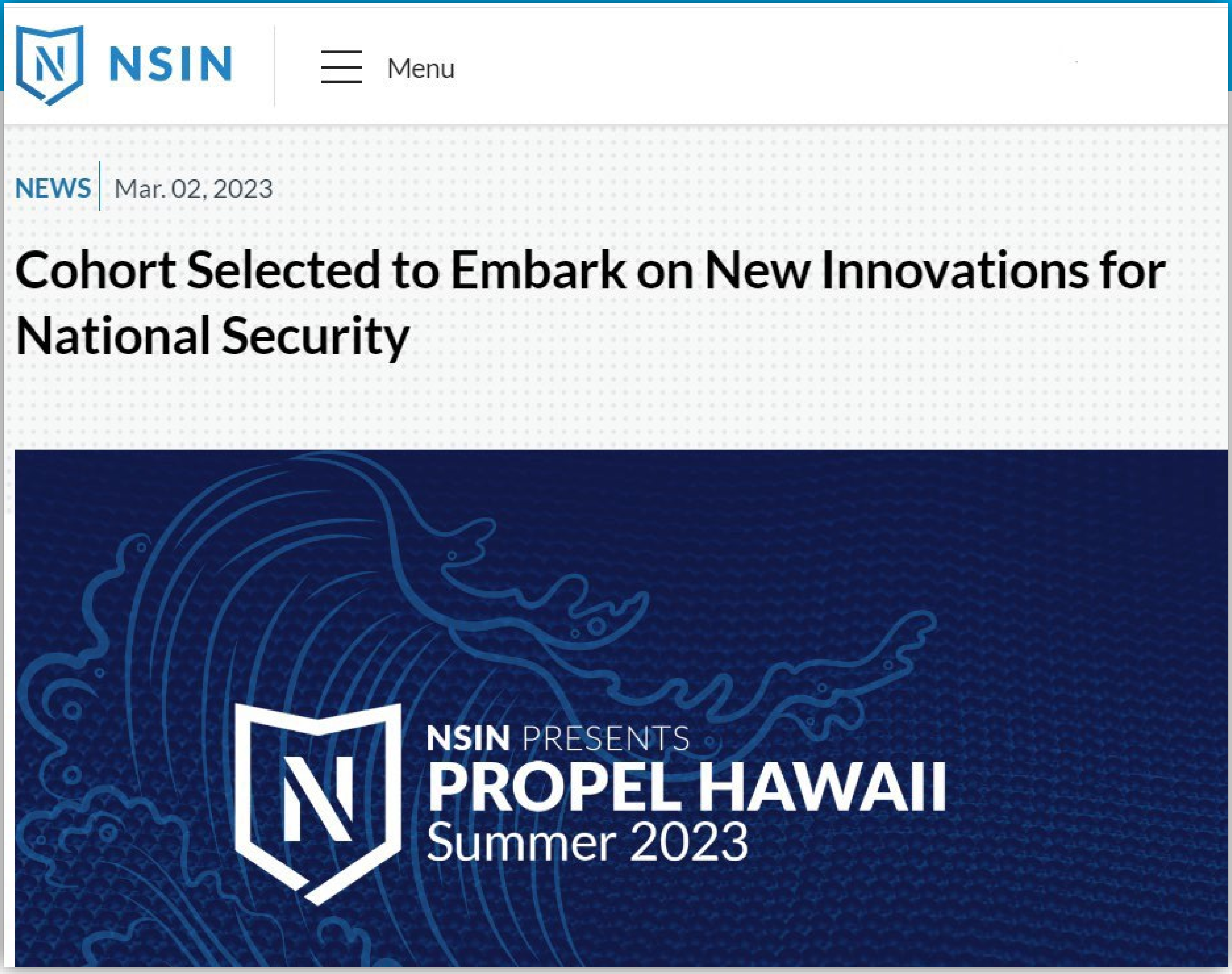
Event description

Having a strong cyber security posture will prepare and position your business to secure contracts with the U.S. Military/DOD/U.S. Navy/ Federal, State Government and within private sector supply chains in FY2023 and beyond.

WIN at small business cybersecurity and protect your contract information and your company!

Understand the industry best practices and how to achieve a secure network for your company.

Be ready to WIN with cybersecurity for your company, your employees and your investment.



NEWS | Mar. 02, 2023

Cohort Selected to Embark on New Innovations for National Security

DAF CISO's Blue Cyber

Social Media Links which each post weekly about Blue Cyber's weekly events

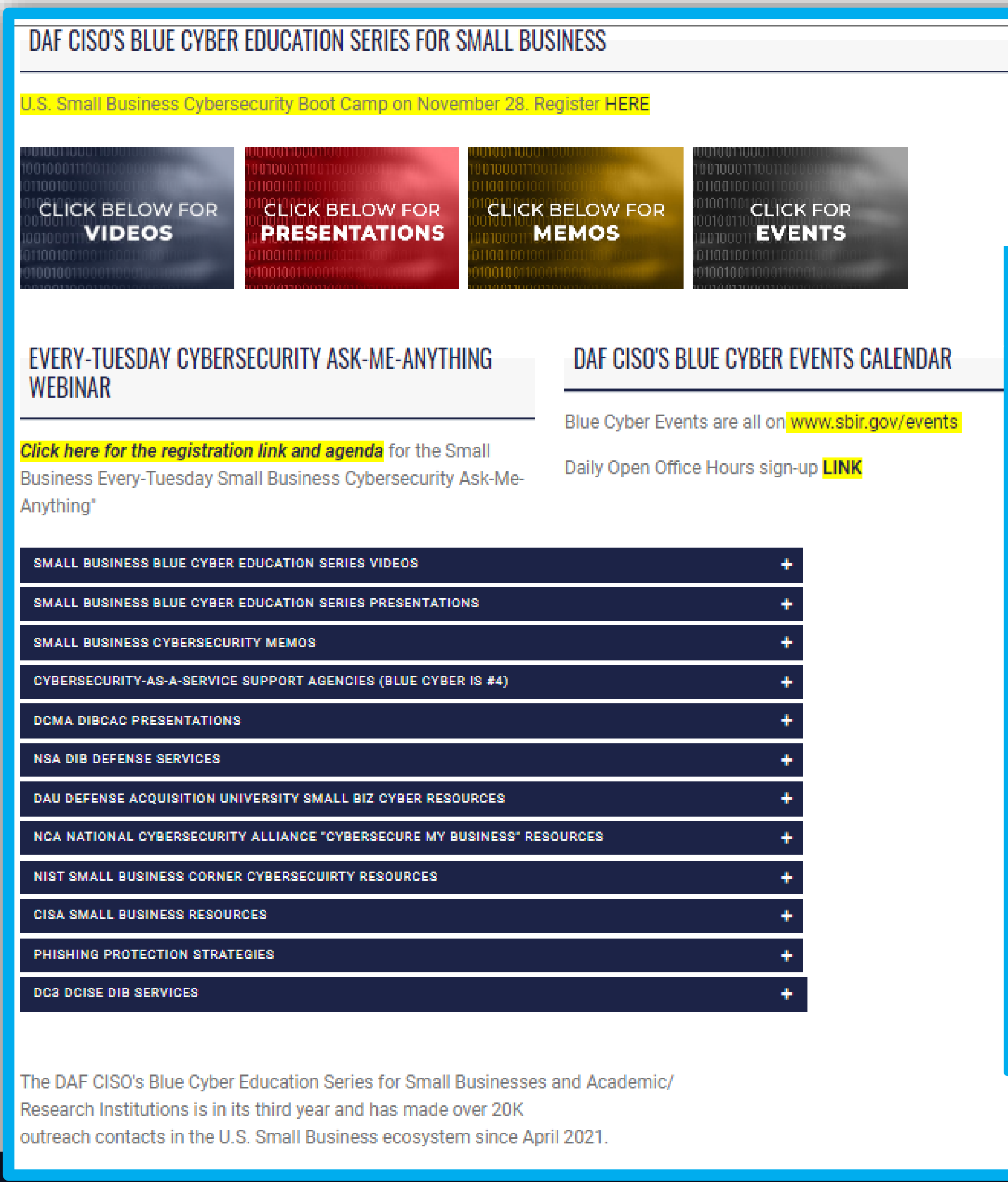
AFWERX SOCIAL MEDIA LINKS

- X/Twitter
- Facebook
- Instagram
- LinkedIn
- YouTube

DAF CISO'S BLUE CYBER

Website
The Blue Cyber Education Series for Small Businesses webpage

Daily Office Hours
We have daily office hours for answering/researching your questions about Small Business cybersecurity and data protection!



DAF CISO'S BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

U.S. Small Business Cybersecurity Boot Camp on November 28. Register HERE

EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING WEBINAR

Click here for the registration link and agenda for the Small Business Every-Tuesday Small Business Cybersecurity Ask-Me-Anything"

DAF CISO'S BLUE CYBER EVENTS CALENDAR

Blue Cyber Events are all on www.sbir.gov/events

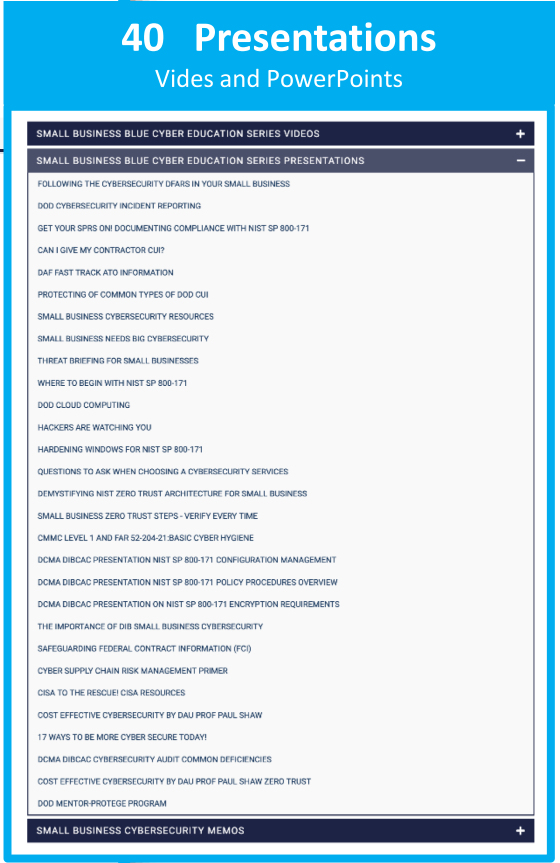
Daily Open Office Hours sign-up LINK

- SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS +
- SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS +
- SMALL BUSINESS CYBERSECURITY MEMOS +
- CYBERSECURITY-AS-A-SERVICE SUPPORT AGENCIES (BLUE CYBER IS #4) +
- DCMA DIBCAC PRESENTATIONS +
- NSA DIB DEFENSE SERVICES +
- DAU DEFENSE ACQUISITION UNIVERSITY SMALL BIZ CYBER RESOURCES +
- NCA NATIONAL CYBERSECURITY ALLIANCE "CYBERSECURE MY BUSINESS" RESOURCES +
- NIST SMALL BUSINESS CORNER CYBERSECUIRTY RESOURCES +
- CISA SMALL BUSINESS RESOURCES +
- PHISHING PROTECTION STRATEGIES +
- DC3 DCISE DIB SERVICES +

The DAF CISO's Blue Cyber Education Series for Small Businesses and Academic/Research Institutions is in its third year and has made over 20K outreach contacts in the U.S. Small Business ecosystem since April 2021.

Events
All FREE and PUBLIC
www.sbir.gov/events

40 Presentations
Vides and PowerPoints

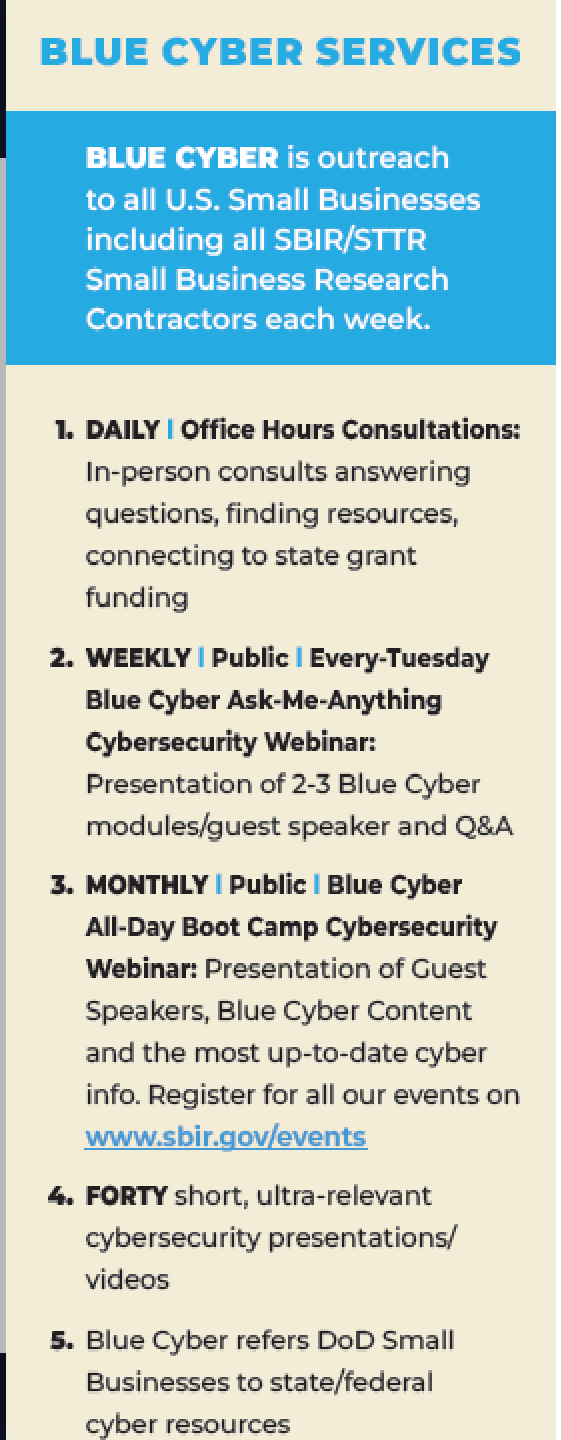


- SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS +
- SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS –
  - FOLLOWING THE CYBERSECURITY DFARS IN YOUR SMALL BUSINESS
  - DOD CYBERSECURITY INCIDENT REPORTING
  - GET YOUR SPRS ON! DOCUMENTING COMPLIANCE WITH NIST SP 800-171
  - CAN I GIVE MY CONTRACTOR CUI?
  - DAF FAST TRACK ATO INFORMATION
  - PROTECTING OF COMMON TYPES OF DOD CUI
  - SMALL BUSINESS CYBERSECURITY RESOURCES
  - SMALL BUSINESS NEEDS BIG CYBERSECURITY
  - THREAT BRIEFING FOR SMALL BUSINESSES
  - WHERE TO BEGIN WITH NIST SP 800-171
  - DOD CLOUD COMPUTING
  - HACKERS ARE WATCHING YOU
  - HARDENING WINDOWS FOR NIST SP 800-171
  - QUESTIONS TO ASK WHEN CHOOSING A CYBERSECURITY SERVICES
  - DEMYSTIFYING NIST ZERO TRUST ARCHITECTURE FOR SMALL BUSINESS
  - SMALL BUSINESS ZERO TRUST STEPS - VERIFY EVERY TIME
  - CMMC LEVEL 1 AND FAR 52-204-21:BASIC CYBER HYGIENE
  - DCMA DIBCAC PRESENTATION NIST SP 800-171 CONFIGURATION MANAGEMENT
  - DCMA DIBCAC PRESENTATION NIST SP 800-171 POLICY PROCEDURES OVERVIEW
  - DCMA DIBCAC PRESENTATION ON NIST SP 800-171 ENCRYPTION REQUIREMENTS
  - THE IMPORTANCE OF DIB SMALL BUSINESS CYBERSECURITY
  - SAFEGUARDING FEDERAL CONTRACT INFORMATION (FCI)
  - CYBER SUPPLY CHAIN RISK MANAGEMENT PRIMER
  - CISA TO THE RESCUE! CISA RESOURCES
  - COST EFFECTIVE CYBERSECURITY BY DAU PROF PAUL SHAW
  - 17 WAYS TO BE MORE CYBER SECURE TODAY!
  - DCMA DIBCAC CYBERSECURITY AUDIT COMMON DEFICIENCIES
  - COST EFFECTIVE CYBERSECURITY BY DAU PROF PAUL SHAW ZERO TRUST
  - DOD MENTOR-PROTEGE PROGRAM
- SMALL BUSINESS CYBERSECURITY MEMOS +

Blue Cyber
Small Biz

Always Free
Always Public

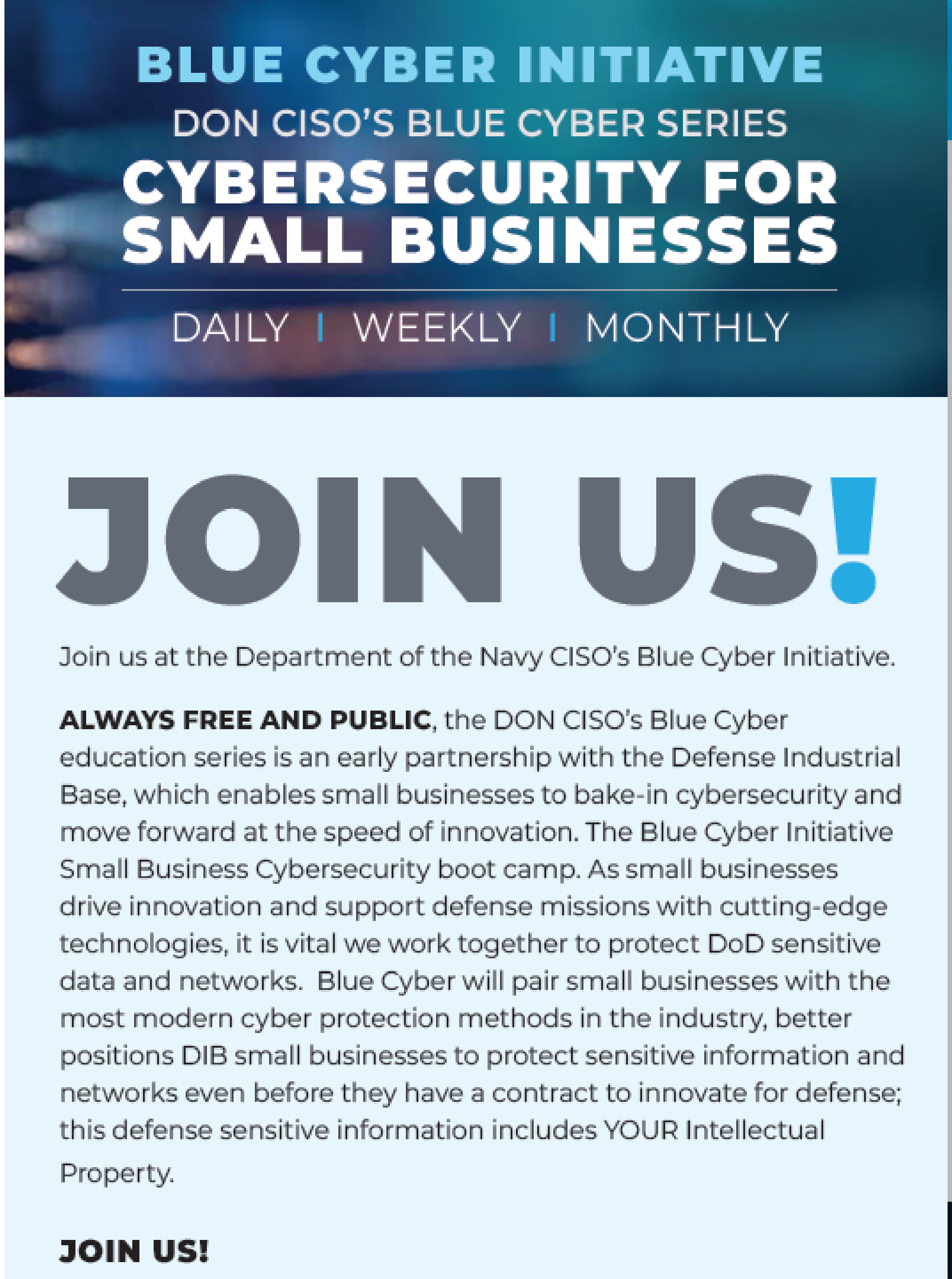
Sign-up at
www.sbir.gov/
events



BLUE CYBER SERVICES

BLUE CYBER is outreach to all U.S. Small Businesses including all SBIR/STTR Small Business Research Contractors each week.

1. **DAILY | Office Hours Consultations:** In-person consults answering questions, finding resources, connecting to state grant funding
2. **WEEKLY | Public | Every-Tuesday Blue Cyber Ask-Me-Anything Cybersecurity Webinar:** Presentation of 2-3 Blue Cyber modules/guest speaker and Q&A
3. **MONTHLY | Public | Blue Cyber All-Day Boot Camp Cybersecurity Webinar:** Presentation of Guest Speakers, Blue Cyber Content and the most up-to-date cyber info. Register for all our events on www.sbir.gov/events
4. **FORTY** short, ultra-relevant cybersecurity presentations/ videos
5. Blue Cyber refers DoD Small Businesses to state/federal cyber resources



BLUE CYBER INITIATIVE

DON CISO'S BLUE CYBER SERIES

CYBERSECURITY FOR SMALL BUSINESSES

DAILY | WEEKLY | MONTHLY

JOIN US!

Join us at the Department of the Navy CISO's Blue Cyber Initiative.

ALWAYS FREE AND PUBLIC, the DON CISO's Blue Cyber education series is an early partnership with the Defense Industrial Base, which enables small businesses to bake-in cybersecurity and move forward at the speed of innovation. The Blue Cyber Initiative Small Business Cybersecurity boot camp. As small businesses drive innovation and support defense missions with cutting-edge technologies, it is vital we work together to protect DoD sensitive data and networks. Blue Cyber will pair small businesses with the most modern cyber protection methods in the industry, better positions DIB small businesses to protect sensitive information and networks even before they have a contract to innovate for defense; this defense sensitive information includes YOUR Intellectual Property.

JOIN US!