DAF CISO’s Small Business Cybersecurity Resources

Lollapalooza
AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO’s
Small Business Cybersecurity Resources
Lollapalooza

New Mexico
APEX Accelerator

Elythia McAnarney

Jan 30, 2024
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
**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
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
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.
DON C IS O'S BLUE CYBER

POWERED BY

Jan 30, 2024

BLUE CYBER EDUCATION SERIES

DAF CISO’s
Small Business Cybersecurity Resources
Lollapalooza

AN OFFERING IN THE BLUE CYBER SERIES

California
NIST MEP Center
CMTC

Chris Buthe

Jan 30, 2024

AFWERX
BLUE CYBER EDUCATION SERIES
Cybersecurity Resources for U.S. Innovation & Manufacturing

Chris Buthe
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

- 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

Success depends on collaboration

RESOURCES: DoD and NIST MEP Resource recommendations
Your Key Partners are your Resources

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?

RESOURCE: https://opr.ca.gov/economic-development/cascade.html
Resources for Innovation Researchers

BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

RESOURCE: www.cmtc.com
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

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

RESOURCES: https://www.nist.gov/mep/cybersecurity-resources-manufacturers
Resources from your NIST Laboratories

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

RESOURCES: 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

RESOURCE: www.cmtc.com
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

RESOURCE: www.cmtc.com
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

RESOURCE: www.cmtc.com
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

CSET
Ransomware Readiness Assessment

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/.
CSET
Ransomware Readiness Assessment

RESOURCE: https://cset-download.inl.gov/.
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
Resources from CADENCE

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

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

READINESS
Capability
Capacity

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)

RESOURCES: 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

I'm interested in...

- Counterintelligence
- Cybersecurity
- General Security
- Industrial Security
- Information Security
- Insider Threat
- Operations Security
- Personnel Security
- Physical Security
- Special Access Programs

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

- Case Studies
- Job Aids
- Games
- Posters
- Security Shorts
- Security Videos
- Toolkits
- Webinars & Conferences

Readiness
Capability
Capacity


RESOURCE: CDSE https://www.cdse.edu
Resources from CISA

SECURING THE SOFTWARE SUPPLY CHAIN
RECOMMENDED PRACTICES GUIDE FOR SUPPLIERS

DON'T WAKE UP TO A RANSOMWARE ATTACK

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 through case studies
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,

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
National Security Agency
Defense Industrial Base Services

Peter DeLuca

Jan 30, 2024
Malicious actors weaponize vulnerabilities 40% faster than defenders remediate them and most organizations remediate less than half of known vulnerabilities.

**Complexity of the DoD Supply Chain**

How Many Contacts Are Truly In Your Network?

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

**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.

**Patch Fatigue & Issue Prioritization**

Project: 500 CVEs published per week in 2025

- The average org has >100,000 backlogged vulnerabilities
- Published in NVD in 2022 – Less than 2% were exploited by malicious actors

**What do you plan to do differently for vulnerability management by 2025? What are you doing now that needs bolstering?**
THREAT-INFORMED DEFENSE

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 MANAGEMENT
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

In some cases, this process can take less than 15 minutes
AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza

NIST
Small Business Corner

Daniel Eliot

Jan 30, 2024

BLUE CYBER EDUCATION SERIES
Overview of NIST Small Business Resources

January 30, 2024
Celebrating 50+ Years in Cybersecurity

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

[nist.gov](http://nist.gov)
Agenda

• NIST Small Business Cybersecurity Corner Website

• Hollings Manufacturing Extension Partnership (MEP)

• NIST Small Business Innovation Research (SBIR) Program

• Additional Resources
Your secure business is just around the corner.
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.

https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics
NIST Cybersecurity Framework (CSF)

CSF Introductory Resources

- NIST’s [Cybersecurity Framework Quick Start Guide](https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework)
- MEP’s [Cybersecurity Framework Steps for Small Manufacturers](https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework)
- FTC’s [Understanding the NIST Cybersecurity Framework](https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework)
Guidance by Topic

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

- **Phishing**
  - Protecting Your Small Business: Phishing
  - See the Phishing companion PDF [here](#).

- **Multi-Factor Authentication**
  - Protecting Your Small Business: Multi-Factor Authentication
  - See the Multi-Factor Authentication companion PDF [here](#).

- **Ransomware**
  - Protecting Your Small Business: Ransomware
  - See the Ransomware companion PDF [here](#).

---

**You've Been Phished**

- Protecting Your Small Business: You've Been Phished

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

---

**The NIST Privacy Framework**

- Protecting Your Small Business: 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

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

https://www.nist.gov/mep
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 Stress 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.
  Manufacturing Extension Partnership

- 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 (DFARS) (FAR)

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

https://www.nist.gov/itl/smallbusinesscyber/events
NIST SBIR Program

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

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
Questions?

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

smallbizsecurity@nist.gov
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.
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 cyber security 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.
DAILY, Open 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 – 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
Everybody Handles Federal Contracting Information!
Walk Through of the FAR 52.204-21 and proposed CMMC Level 1

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/
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.
If you are a DOD contractor, You must report cyber incidents to DC3
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
The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry.

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!
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:
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!

Find a Mentor ▶️

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.

Take The Series ▶️
FCC CYBER PLANNING GUIDE

- 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

www.fcc.gov/cyberplanner
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.
CUI References:
- Executive Order 13556, November 4, 2010
- 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](https://www.dcma.mil/DIBCAC/) 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.
Local Assistance

www.sbir.gov/local-assistance
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
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.doucier@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.

Register
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
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!

Events
All FREE and PUBLIC [www.sbir.gov/events](http://www.sbir.gov/events)

40 Presentations
Videos and PowerPoints
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

Always Free
Always Public

Sign-up at www.sbir.gov/events

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!