

AN OFFERING IN THE BLUE CYBER SERIES

# Small Business Needs BIG CYBERSECURITY



VERSION: JUNE 2023

#9 IN THE DON CISO's BLUE CYBER EDUCATION SERIES



# DON CISO'S BLUE CYBER

POWERED BY



## BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

CLICK FOR VIDEOS

CLICK FOR PRESENTATIONS

CLICK FOR MEMOS

CLICK FOR EVENTS

### EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING

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

### BLUE CYBER EVENTS CALENDAR

Blue Cyber Events are all on [www.sbir.gov/events](http://www.sbir.gov/events)

Open Office Hours for sign-up [LINK](#)

SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS +

SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS +

SMALL BUSINESS CYBERSECURITY MEMOS +

### QUICK LINKS

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

The Blue Cyber Education Series for Small Businesses and Academic/ Research Institutions is in its second year and has made over 13K outreach contacts in the U.S. Small Business ecosystem since April 2021.

Blue Cyber is dedicated to an early-partnership with Defense Industrial Base small business contractors and potential contractors arm them with the latest in cybersecurity best practices.

**Every Day** there are FREE-PUBLIC office hours with SBIR/STTR and small business firms, to connect them to resources and answer their questions. Sign up for Open Office Hours [HERE](#)

**Every Tuesday** FREE-PUBLIC Cybersecurity Ask-Me-Anything webinars at 1pm Eastern;

**Every Month** A FREE-PUBLIC all-day boot camp

**40 FREE modules** on cybersecurity and information protection with links to all the Blue Cyber events

## 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
- NIST SP 800-171 POLICY PROCEDURES OVERVIEW
- QUESTIONS TO ASK WHEN CHOOSING A CYBERSECURITY SERVICES
- CMMC 2.0 EXPLAINED
- 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 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

SMALL BUSINESS CYBERSECURITY MEMOS +

## The Slides are Located at:

[www.safcn.af.mil/  
CISO/Small-Business-  
Cybersecurity-  
Information/](http://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/)



# Big Cybersecurity

- The “Why” for Big Cybersecurity for Small Businesses
- Execute the DFARS requirements
- Report Cyber Incidents
- Protect Controlled Unclassified Information(CUI) – and your Intellectual Property!
- Implement NIST SP 800-171
- Get your SPRS On!
- Share CUI when you are ready to protect it
- Get all the help available to the DIB Small Business community



# The Importance of Cybersecurity for Department of the Navy Small Businesses

As small businesses drive innovation and support the Department of the Navy (DON) missions with cutting-edge technologies, it is vital we work together to protect DON sensitive data and networks. Failure to protect our sensitive data will put service members and military missions at risk. We must match the aggressiveness of our cyber adversaries with radical teamwork to bring our small businesses up-to-speed in the most modern methods for comprehensive protection of DON sensitive data and networks.

The DON CISO Office Blue Cyber education series is the early partnership with the Defense Industrial Base (DIB) which enables small businesses to bake-in cybersecurity and move forward at the speed of innovation. Pairing small businesses with the most modern cyber protection methods in the industry, better positions DIB small businesses to protect sensitive information and networks just soon as they have a contract to innovate for the DON. Small businesses are equally vulnerable to cyber threats and may have fewer resources than larger businesses with which to counter cyber threats. The key to protecting our DON Sailors and Marines in the exercise of their missions is getting an early start embracing our common cybersecurity and data protection goals by working together to create layered cyber defenses for the DIB small businesses.

This presentation will take you through the vital areas of cybersecurity collaboration for small businesses.



Flows down to  
Subcontractors

# Federal Acquisition Regulation (FAR) and DFARS

Small Business contracts contains many FARs and DFARS, you must study them at length. These are not all of them, but these are some key security requirements.

What is a DFARS? The Defense Federal Acquisition Regulation Supplement (**DFARS**) contains requirements of **law**, DoD-wide policies, delegations of Federal Acquisition Regulation (**FAR**) authorities, deviations from **FAR** requirements, and policies/procedures that have a significant effect on the public.

DFARS Clause  
252.239-7010  
Cloud Computing  
Services

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

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

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

DFARS Clause  
252.204-  
7019/7020  
NIST SP 800-171  
DoD Assessment  
Requirements.

DFARS Clause  
252.204-7021  
Cybersecurity  
Maturity Model  
Certification  
Requirement

DFARS Clause  
252.204-7024  
Use of  
Supplier  
Performance Risk  
System (SPRS)  
Assessments



## DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirement

This DFARS is under review and it's status will not be known until early 2023 at the earliest.

Until then, compliance with and full implementation of DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" is sufficient.


For more information on the new version of CMMC, see this great webinar by the DCMA Director John Ellis.

<https://www.preveil.com/resources/webinar-john-ellis-on-cmmc-2-0/>

Stay up-to-date at [www.acq.osd.mil/cmmc/](http://www.acq.osd.mil/cmmc/)



<https://dodcio.defense.gov/CMMC/>



**CHIEF INFORMATION OFFICER**  
U.S. DEPARTMENT OF DEFENSE

Search Chief Information 🔍

HOME
ABOUT DOD CIO ▾
IN THE NEWS
LIBRARY
CMMC ▾
CONTACT US

**UPDATES TO THE CMMC WEBSITE WILL BE LIMITED DURING THE CMMC 2.0 RULEMAKING PROCESS**


## CYBERSECURITY MATURITY MODEL CERTIFICATION

---


**CMMC 2.0**

To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base's (DIB) sensitive unclassified information from frequent and increasingly complex cyberattacks. With its streamlined requirements, CMMC 2.0:

- Simplifies compliance by allowing self-assessment for some requirements
- Applies priorities for protecting DoD information
- Reinforces cooperation between the DoD and industry in addressing evolving cyber threats




**CMMC 2.0 LAUNCHED**




Senior Department leaders announce the strategic direction and goals of CMMC 2.0

LEARN MORE




**CMMC 2.0 PROGRAM**




What you need to know about the program and what's changed from CMMC 1.0

LEARN MORE



**5 STEPS TO CYBERSECURITY**



Actions your company can take today to protect against cyber threats

LEARN MORE



## DFARS Clause 252.239-7010 – Cloud Computing Services

Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud

**Ensures** that the cloud service provider:

- Meets requirements of the DoD Cloud Computing Security Requirements Guide
- Use government-related data only to manage the operational environment that supports the Government data and for no other purpose
- Complies with requirements for cyber incident reporting and damage assessment

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, applies when a contractor intends to use an external cloud service provider to store, process, or transmit covered defense information in the performance of a contract. DFARS Clause 252.204-7012 requires the cloud service provider to meet security requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.





## FAR Clause 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

### **Safeguarding Requirements and Procedures**

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- The FAR lists 15 security controls, which are considered basic cyber hygiene

(2) *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

### **Flow-Down the Requirement**

The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.



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



Report cyber incidents



Submit malicious software



Facilitate damage assessment



Safeguard covered defense information



# What if There is a Potential Breach?

**Don't Panic.** Cybersecurity occurs in a dynamic environment. Hackers are constantly coming up with new ways to attack information systems, and DoD is constantly responding to these threats. Even if a contractor does everything right and institutes the strongest checks and controls, it is possible that someone will come up with a new way to penetrate these measures. DoD does not penalize contractors acting in good faith. The key is to work in partnership with DoD so that new strategies can be developed to stay one step ahead of the hackers.

**Contact DoD Immediately.** Bad news does not get any better with time. These attacks threaten America's national security and put service members' lives at risk. DoD has to respond quickly to change operational plans and to implement measures to respond to new threats and vulnerabilities. Contractors should report any potential breaches to DoD **within 72 hours of discovery of any incident.**

**Be Helpful and Transparent.** Contractors must also cooperate with DoD to respond to security incidents. Contractors should immediately preserve and protect all evidence and capture as much information about the incident as possible. They should review their networks to identify compromised computers, services, data and user accounts and identify specific covered defense information that may have been lost or compromised.



# What to Report to the Federal Government

**DHS Definition:** A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.

**DFARS 7012 Definition** “Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.



# Where to Report Cyber Incidents/Malware



To report cyber incidents that affect covered defense information **OR** that affect the contractor's ability to perform requirements designated as operationally critical support, the Contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DoD at <https://dibnet.dod.mil> via an incident collection form (ICF).



If discovered and isolated in connection with a reported cyber incident, the contractor/subcontractor shall submit the malicious software to the DoD Cyber Crime Center (DC3). Also, <https://dibnet.dod.mil>



If DoD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to request media and damage assessment information from the contractor



# 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](#)

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



A FEDERAL CYBER CENTER

# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

7 Jun 23

## Cyber Threat Roundup

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

### Contents

Articles ..... 2

- New ChatGPT Attack Technique Spreads Malicious Packages ..... 2
- Multiple Vulnerabilities in Mozilla Products Could Allow for Arbitrary Code Execution ..... 2
- Outlook.com Hit by Outages as Hacktivists claim DDoS Attacks ..... 2
- Malicious Chrome Web Store Extensions Identified ..... 2



# Safeguard Covered Defense Information (CDI)



CDI is defined as unclassified controlled technical information (CTI) or other information as described in the DOD CUI Registry

**AND** it is marked as CUI

---

**OR** otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract;

---

**OR** collected/developed/received/transmitted/used/ stored by the contractor in performance of contract.





# Safeguard CDI: What is CUI?



The DOD CUI Registry and detailed training on what constitutes CUI is available from the DOD at this link:

<https://www.dodcui.mil>

DoD Controlled Unclassified Information (CUI)

DEPARTMENT OF DEFENSE  
UNITED STATES OF AMERICA

## CUI Awareness and Marking

November 2020

<https://www.dodcui.mil>

CLEARED  
For Open Publication  
Apr 01, 2021

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

**SLIDES ONLY  
NO SCRIPT PROVIDED**

21-S-0588



# Safeguard CDI: What is CTI?



Controlled Technical Information (CTI) means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Controlled technical information is to be marked.

The term does not include information that is lawfully publicly available without restrictions.

"Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items"

**Examples of technical information include: research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.**



# Implementation of NIST SP 800-171

**Implementation** of the NIST SP 800-171 involves implementing and documenting the 110 security requirements listed in the document.

- The implementation of security requirements is recorded in a System Security Plan (NIST SP 800-171 security requirement 3.12.4) and
- Any un-implemented security requirement and its interim plan to provide alternative, but equally effective, security measure is recorded in a Plan of Action with Milestones, called a POAM (NIST SP 800-171 security requirement 3.13.2)

Help with understanding the NIST SP 800-171 security requirements is found at this link:

<https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>



# NIST SP 800-171 System Security Plan (SSP)

<<Insert name>> SYSTEM SECURITY PLAN Last Updated: <<Insert date>>

---

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: [Insert the System Unique Identifier]

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI):

Name:	
Title:	
Office Address:	

Optional Template  
available on NIST.Gov

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will be achieved

Optional Template to record the  
Plan of Action on NIST.gov



# Safeguard Covered Defense Information (CDI)



To safeguard covered defense information contractors/subcontractors **must implement NIST SP 800-171**, Protecting CUI in Nonfederal Information Systems and Organizations

The covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171

- The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.
- The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO



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

**States** “By submission of this offer, the Offeror represents that it will implement the security requirements specified by NIST SP 800-171, ... not later than December 31, 2017.

**If the Offeror proposes to vary** from any of the security requirements specified by NIST SP 800-171 ..., the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of:

- Why a particular security requirement is not applicable
- How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.
- An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing **prior to contract award**. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.



# The Requirement in DFARS Clause 252.204-7019/7020 - NIST SP 800-171 DoD Assessment Requirements

In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment for each covered contractor information system that is relevant to the contract.

A Basic Assessment, which is a self-assessment assigned a low confidence level (because it is self-generated) is:

- Based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s)
- Conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology



# Not All of the NIST SP 800-171 Security Requirements are Equal

The NIST SP 800-171 DoD Assessment Methodology identifies **42 security requirements** that, if not implemented, could lead to **significant exploitation of the network, or exfiltration of DoD CUI.**

These high-risk security requirements are with 5 points in the DoD scoring rubric.

- For example, Failure to limit system access to authorized users (Requirement 3.1.1) **renders all the other Access Control requirements ineffective, allowing easy exploitation of the network**
- For example, Failure to control the use of removable media on system components (Requirement 3.8.7) **could result in massive exfiltration of CUI and introduction of malware.**

*NIST SP 800-171 DoD Assessment Scoring Template*

	Security Requirement	Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

12





DFARS Clause 252.204-7019/7020  
NIST SP 800-171 DoD Assessment Requirements.



Self-Assessment



Submit information to [SPRS.CSD.DISA.MIL](mailto:SPRS.CSD.DISA.MIL)



Flow the Requirement Down



Update your Self-Assessment

NIST SP 800-171



# How to Enter a Basic Assessment Data into SPRS

Post or email your business' summary level scores of a current NIST SP 800-171 DoD Assessment to SPRS for all covered contractor information systems relevant to the contract.

Your entry consists of

- 1. A system security plan** (NIST SP 800-171 item 3.12.4) supporting the performance of a DoD contract—)
- 2. Summary level score** (e.g., 95 out of 110, NOT the individual value for each requirement) using the NIST SP 800-171 DoD Assessment Methodology
- 3. Date that all requirements are expected to be implemented** (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171

The SPRS website offers numerous training videos which will help you get an account and make your entry





# How to enter a Basic Assessment Data into SPRS

**NIST SP 800-171 ASSESSMENT**

**Enter Assessment Details**

Assessment Date:

Score:

Assessing Scope:

Plan of Action Completion Date:

System Security Plan (SSP) Assessed:

SSP Version/Revision:

SSP Date:

Included CAGE(s):

Include HLO

SPRS Basic Assessment data entry fields

**ELECTRONICS, INC.** - [Show Less Detail](#) [\(Return to Top\)](#)

Most Rec... Assessm...	Assess... Score	Confidence Level	Assessm... Standard	Assessin... or DoDA...	Scope	Included CAGEs/entities	Plan of A... Completi...	System Se... System Se...	SSP Ve... SSP Ve...	SSP Date
04/06/2019	109	BASIC	NIST SP 800-171		ENTERPRISE	ELECTRONICS, INC. USA	07/30/2021	Network Security Plan		03/01/2019

1

Example output  
of SPRS Basic Assessment



# You Have Help with the new DOD CIO documents

## Access Control (AC)

### Level 1 AC Practices

#### AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

#### ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

- [a] authorized users are identified;
- [b] processes acting on behalf of authorized users are identified;
- [c] devices (and other systems) authorized to connect to the system are identified;
- [d] system access is limited to authorized users;
- [e] system access is limited to processes acting on behalf of authorized users; and
- [f] system access is limited to authorized devices (including other systems).

#### POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

##### Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

##### Interview

[SELECT FROM: Personnel with account management responsibilities; system or network

#### DISCUSSION [NIST SP 800-171 R2]

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged versus *[sic]* non-privileged) are addressed in requirement 3.1.2 (AC.L1-3.1.2).

#### FURTHER DISCUSSION

Identify users, processes, and devices that are allowed to use company computers and can log on to the company network. Automated updates and other automatic processes should be associated with the user who initiated (authorized) the process. Limit the devices (e.g., printers) that can be accessed by company computers. Set up your system so that only authorized users, processes, and devices can access the company network.

This practice, AC.L1-3.1.1, controls system access based on user, process, or device identity. AC.L1-3.1.1 leverages IA.L1-3.5.1 which provides a vetted and trusted identity for access control.

##### Example 1

Your company maintains a list of all personnel authorized to use company information systems [a]. This list is used to support identification and authentication activities conducted by IT when authorizing access to systems [a,d].

##### Example 2

A coworker wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network and will prevent network access by unauthorized systems and devices [c]. You help the coworker submit a ticket that asks for the printer to be granted access to the network, and appropriate leadership approves the device [f].

#### Potential Assessment Considerations

- Is a list of authorized users maintained that defines their identities and roles [a]?
- Are account requests authorized before system access is granted [d,e,f]?<sup>3</sup>

#### KEY REFERENCES



# New Documentation Guides

<https://dodcio.defense.gov/CMMC/>

**ACQUISITION & SUSTAINMENT**  
Office of the Under Secretary of Defense

Home About Model Assessments Implementation Documentation Resources

✓  
**CMMC HELPFUL LINKS**  
 This page contains a variety of external links to CMMC resources throughout the DoD.

✓  
**STILL CAN'T FIND IT?**  
 Contact us directly by e-mail:  
[OSD.AS-Webmaster@mail.mil](mailto:OSD.AS-Webmaster@mail.mil)  
**Standard Operating Hours**  
 Monday - Friday (8am - 5pm)

**MODEL OVERVIEW**

- [Link to Model Overview](#)
- [CMMC 2.0 Spreadsheet and Mapping](#)
- [Link to CMMC Glossary](#)

**SCOPING GUIDANCE**

- [Link to CMMC Level 1 Scoping Guidance](#)
- [Link to CMMC Level 2 Scoping Guidance](#)

**ASSESSMENT GUIDES**

- [CMMC Level 1 Self-Assessment Guide](#)
- [CMMC Level 2 Assessment Guide](#)
- [CMMC Level 3 Assessment Guide: Under Development](#)

**CMMC ARTIFACT HASHING TOOL USER GUIDE**

- [Link to Document](#)



# Why NIST SP 800-171 - Protecting CUI in Nonfederal Information Systems and Organizations?

The NIST SP 800-171 was written using performance-based security requirements to enable contractors to use systems and practices they already have in place to process, store, or transmit CUI.

- It eliminates unnecessary specificity and includes only those security requirements necessary to provide adequate protection.
- Though most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, some require security-related software or additional hardware.



# Can I Give My Contractor CUI?

## DFARS 7012 “Adequate Security” Quote

... (b) *Adequate security.* The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor **shall implement, at a minimum, the following information security protections:**

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system **shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171**, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor **shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017...**



# Answer Today: Can I Give My Contractor CUI? You Need to Ask.

## Yes, if:

- The decision to share CUI is a risk-based decision based upon a conversation with the contractor regarding if they are ready to provide adequate protection to DoD CUI.
- There is not a cut and dried answer rubric.
- CUI protection is a shared responsibility between the DoD and industry.
- Adequate security will vary depending on the nature and sensitivity of the information on any given non-DoD information system.

See DFARS 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting, December 2019,” “Section b”, for a description of “Adequate Security”

If you need help with this decision, please contact your Program or Wing cybersecurity office. Also, Kelley Kiernan from the DON CISO Office is available to talk with you. **Keep your contracting officer informed of your activities.**

This question is being studied across the DOD – check back for an updated answer





# Discuss with the Contractor Their Readiness to Provide Adequate Protection for DOD CUI

## Risk-Based Decision Questions

- Review the contractor's System Security Plan and associated POAM
  - Are all 42, 5-point weighted security requirements implemented with no POAM?
  - Are all 14, 3-point weighted security requirements implemented with no POAM?
- Is the CUI that the DON is considering sharing with the contractor in a sensitive category such as these categories? NOFORN, FED ONLY, NOCON, DL ONLY, REL TO [USA, LIST], DISPLAY ONLY, Attorney-Client, Attorney-WP or otherwise sensitive?
- Is the CUI that the DON is considering sharing with the contractor mission-essential?
- Is the CUI the DON is considering sharing with the contractor appropriate for research?
- Have you rejected the use of synthetic data in this contract?
- Apply these questions to contractor-created CUI and the government-provided CUI



## DFARS 252.204-7024

### Use of Supplier Performance Risk System (SPRS) Assessments



Item Risk



Price Risk



Supplier Risk



Overall Risk



# DOD SAFE Creates Potential Exposure

DOD Safe will let a CAC-holder send CUI to any email address. You must ask contractors if they are ready to provide adequate protection to any CUI sent via DOD SAFE and be satisfied with the answer you receive.

- Contractors who are not ready to protect CUI should not accept CUI

The screenshot shows the DoD SAFE website interface. At the top left is the DoD SAFE logo. At the top right, it says "Logged on as user: KIER...". Below the logo is a navigation bar with icons and labels for Home, Drop-Off, Request a Drop-Off, Pick-up, Outbox, Help, and Logout. The main content area features a list of expandable sections:

- + What is DoD SAFE?
- + What credentials are accepted?
- + What credentials are not accepted?
- + Problems accessing the DoD SAFE site by non-CAC users
- Sending Files

Below the "Sending Files" section, a text box states: "Authenticated CAC users can send files to any email address (i.e., .mil, .gov, .com). Guests (i.e., PIV holders, users with .com and .edu emails) can send files to CAC users." Below this text is a "DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited." watermark.



# What is an Authorization to Operate?

An ATO is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

ATOs often have conditions and assumptions, which must be continuously monitored by the Program Office which applied for the ATO.



# Let's Start at the Beginning: Risk Management Framework (RMF)

- The Risk Management Framework (RMF) is criteria that describe processes for the architecture, security and monitoring of United States government IT systems.
- Created by the Department of Defense, the RMF was adopted by all US federal information systems in 2010. The RMF has been documented by the National Institute of Standards and Technology (NIST) and it serves as the foundation for federal data security strategy.
- RMF requires secure data governance systems and performance of threat modeling to identify cyber risk areas.



# RMF Steps

## Prepare

Essential activities to **prepare** the organization to manage security and privacy risks

## Categorize

**Categorize** the system and information processed, stored, and transmitted based on an impact analysis

## Select

**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)

## Implement

**Implement** the controls and document how controls are deployed

## Assess

**Assess** to determine if the controls are in place, operating as intended, and producing the desired results

## Authorize

Senior official makes a risk-based decision to **authorize** the system (to operate)

## Monitor

Continuously **monitor** control implementation and risks to the system

<https://csrc.nist.gov/projects/risk-management/about-rmf>

# Do I Need an ATO?

# Maybe Not...

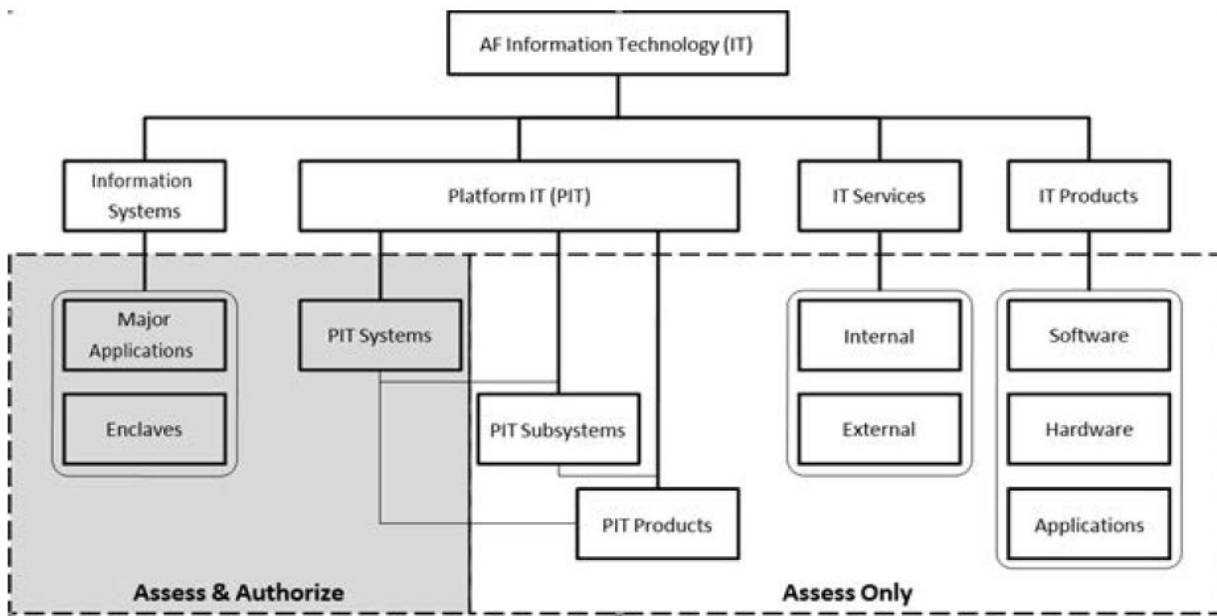


Figure 1: DAF Information Technology (IT)

Reference: AFI 17-101, Fig.1.1. DAF IT Categories

If the Program is proposing an internal or external IS service, such as a web-based application or SaaS, the AO will decide

IT below the system level (Single Purpose IT Products or Devices, PIT Subsystems, PIT Products, IT Products, and IT Services) or if the IS in an internal or external IS service, the AO has discretion to simply approve for use.

 [SEARCH](#)

[FIND A MENTOR](#) [TAKE A WORKSHOP](#) [BROWSE THE LIBRARY](#) [VOLUNTEER](#) [OUR IMPACT](#) [ABOUT US](#)



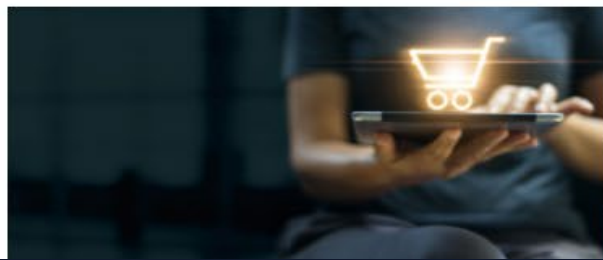
## Small Business Help From SCORE

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 ▶](#)



# MANUFACTURING EXTENSION PARTNERSHIP (MEP)

MEP is a public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers. Last year, MEP Centers interacted with 27,574 manufacturers, leading to \$13.0 billion in sales, \$2.7 billion in cost savings, \$4.9 billion in new client investments, and helped create or retain 105,748 jobs.



MEP • MANUFACTURING  
EXTENSION PARTNERSHIP®

- ABOUT NIST MEP +
- MEP NATIONAL NETWORK +
- EXECUTIVE ORDER 14005
- SUPPLIER SCOUTING
- CYBERSECURITY RESOURCES FOR MANUFACTURERS +
- MATTR
- MANUFACTURING INFOGRAPHICS +
- MANUFACTURING REPORTS
- MANUFACTURING DAY
- MANUFACTURING INNOVATION BLOG
- CONTACT US

## www.nist.gov/mep

[Coronavirus: Resources, Updates, and What You Should Know](#)

HOW THE NETWORK HELPS  
MANUFACTURERS

CONNECT WITH YOUR LOCAL  
MEP CENTER

SUPPLIER SCOUTING

EXECUTIVE ORDER 14005 ON ENSURING THE FUTURE IS MADE IN ALL OF AMERICA BY ALL OF AMERICA'S WORKERS

ALL 51 MEP CENTERS HELPING U.S. MANUFACTURERS MAKE SUCH THINGS AS PPE FROM THE \$50M APPROPRIATED BY CONGRESS

CONNECT WITH US



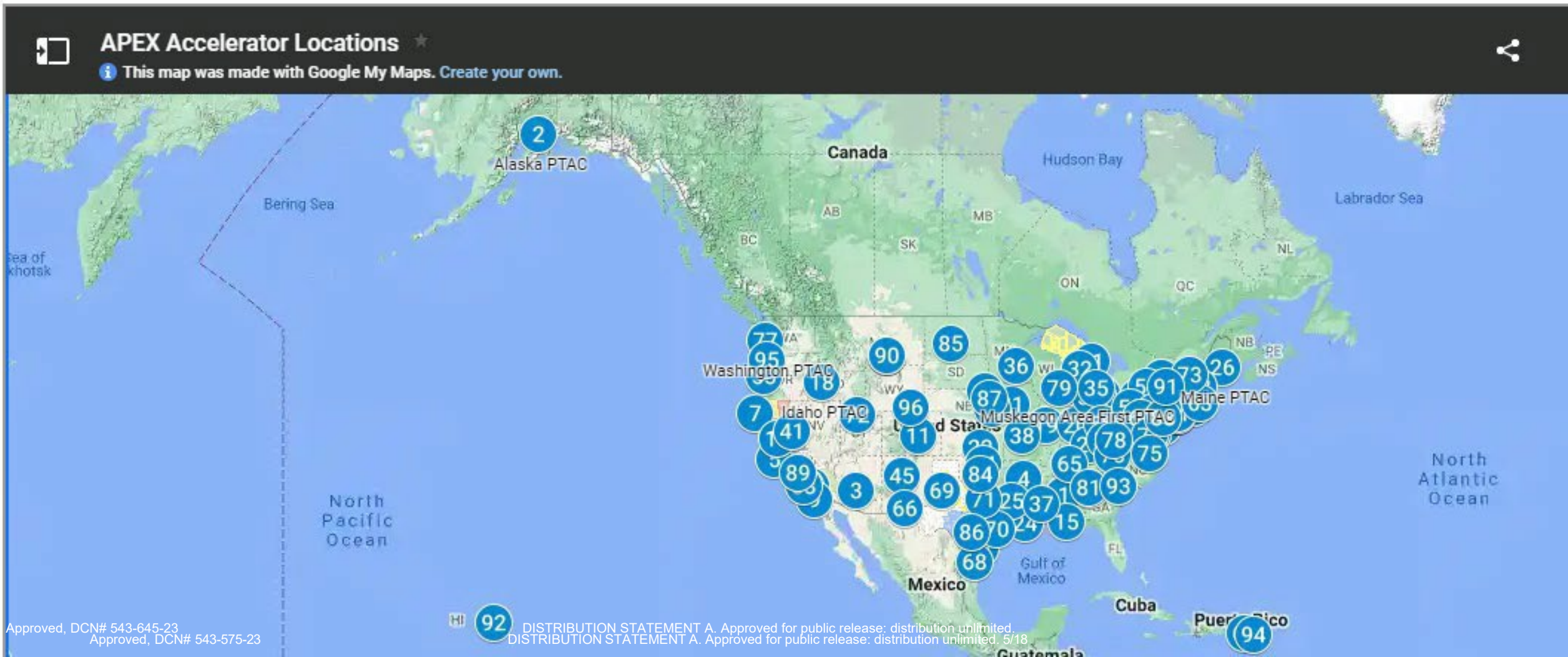
### MANUFACTURING VIDEOS: REAL STORIES, REAL RESULTS

# APEX ACCELERATORS

(Please click on the **drawer icon** in the **left corner of the map** to expand the list of APEX Accelerators, counties in all states, and find direction to your nearest APEX Accelerator by clicking the dot in the interactive map.)

There are more than 90 APEX Accelerators, formerly known as PTACs, assisting businesses in 49 states, Washington, D.C., Puerto Rico, Guam, the U.S. Virgin Islands, the Commonwealth of Northern Marianas, and in regions established by the Department of the Interior of Indian Affairs in the U.S. Department of the Interior.

[www.apexaccelerators.us](http://www.apexaccelerators.us)





# 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

<https://www.fcc.gov/sites/default/files/cyberplanner.pdf>





# DON CISO'S BLUE CYBER







POWERED BY



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


 **CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY** 

Search  [cisa.gov/uscert](#) [Report Cyber Issue](#) [Subscribe to Alerts](#)

 CYBERSECURITY  INFRASTRUCTURE SECURITY  EMERGENCY COMMUNICATIONS  NATIONAL RISK MANAGEMENT  ABOUT CISA  MEDIA

## SHIELDS UP

# SHIELDS UP



Russia's invasion of Ukraine could impact organizations both within and beyond the region, to include **malicious cyber activity** against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners. Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks. **Every organization—large and small**—must be prepared to respond to disruptive cyber incidents. As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

**Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to [report@cisa.gov](mailto:report@cisa.gov) or (888) 282-0870.**

# DON CISO'S BLUE CYBER

POWERED BY



The screenshot displays the top portion of the CISA website. At the top left, the text 'CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY' is accompanied by the CISA seal. To the right, the text 'AMERICA'S CYBER DEFENSE AGENCY' is displayed. A search bar is located in the top right corner. Below the header is a dark blue navigation bar with links for 'Topics', 'Spotlight', 'Resources & Tools', 'News & Events', 'Careers', and 'About'. A red button labeled 'REPORT A CYBER ISSUE' is positioned on the right side of this bar. Below the navigation bar, there is a 'Home' link and social media sharing icons for Facebook, Twitter, LinkedIn, and Email. The main content area features a large blue graphic with circular patterns. A white box is overlaid on the bottom of the graphic, containing the title 'Cross-Sector Cybersecurity Performance Goals' and a blue double-headed arrow below it.



# Cybersecurity Services

TLP:WHITE

## CISA Cybersecurity Services

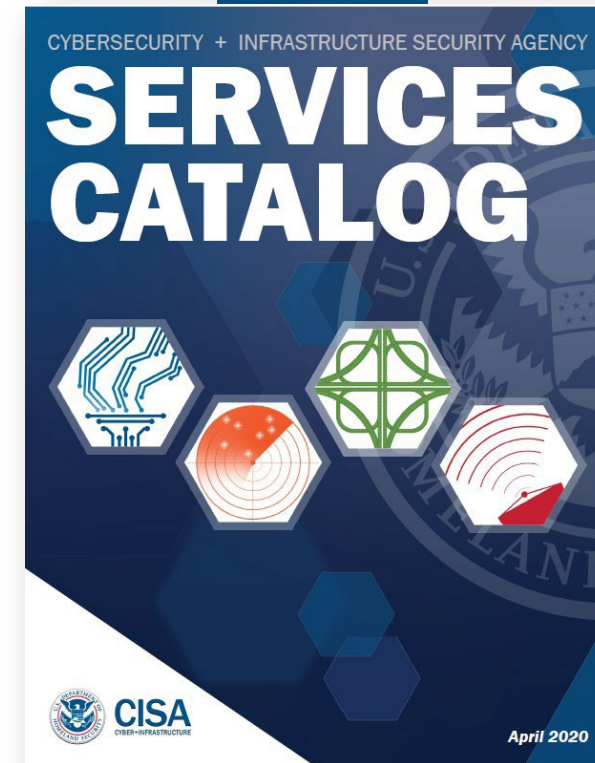
- Vulnerability Scanning
- Remote Penetration Testing
- Phishing Campaign Assessment
- Web Application Scanning
- External Dependencies Management
- Cyber Resilience Review
- & more

For more information on these services, visit

[www.cisa.gov/publication/cisa-services-catalog](https://www.cisa.gov/publication/cisa-services-catalog)

-OR-

<https://www.cisa.gov/cyber-resource-hub>



J.D. Henry  
April 18, 2022

11



# When it's Time to Get Strong Anti-Virus

This screenshot shows the top portion of the CISA website. At the top left is the CISA logo and the text 'CYBERSECURITY &amp; INFRASTRUCTURE SECURITY AGENCY'. To the right is a search bar and a 'cisa.gov/uscert' button. Below the header is a navigation menu with icons for CYBERSECURITY, INFRASTRUCTURE SECURITY, EMERGENCY COMMUNICATIONS, NATIONAL RISK MANAGEMENT, ABOUT CISA, and MEDIA. The main content area features a large blue banner with a yellow starburst graphic containing the word 'FREE' in large letters, followed by the text 'CYBERSECURITY SERVICES AND TOOLS'.

[www.cisa.gov/free-cybersecurity-services-and-tools](http://www.cisa.gov/free-cybersecurity-services-and-tools)

This screenshot shows a specific security tip page on the CISA website. The header includes the CISA logo and navigation links for Alerts and Tips, Resources, and Industrial Control Systems. The page title is 'Security Tip (ST04-005) Understanding Anti-Virus Software'. Below the title is the original release date (June 30, 2009) and the last revised date (September 27, 2019). There are social media sharing buttons for Print, Tweet, Send, and Share. The main text explains what anti-virus software does, noting that it scans files and memory for malicious software (malware). A blue callout box on the right states: 'Anti-virus software can identify and block many viruses before they can infect your computer. Once you install anti-virus software, it is important to keep it up to date.' The text continues with advice to scan the entire computer periodically and lists two types of scans: automatic scans and manual scans.

[www.cisa.gov/uscert/ncas/tips/ST04-005](http://www.cisa.gov/uscert/ncas/tips/ST04-005)



# When it's Time to Get Strong Anti-Virus

## Reducing the Likelihood of a Damaging Cyber Incident

Service	Skill Level	Owner	Description	Link
Immuneset <b>Antivirus</b>	Basic	Cisco	Immuneset is a malware and <b>antivirus</b> protection system for Microsoft Windows that utilizes cloud computing to provide enhanced community-based security.	<a href="https://www.immuneset.com/">https://www.immuneset.com/</a>
Microsoft Defender <b>Antivirus</b>	Basic	Microsoft	This tool is used to protect and detect endpoint threats including file-based and fileless malware. Built into Windows 10 and 11 and in versions of Windows Server.	<a href="https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows">https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows</a>
ClamAV	Advanced	Cisco	ClamAV is an open-source (general public license [GPL]) <b>antivirus</b> engine used in a variety of situations, including email and web scanning, and endpoint security. It provides many utilities for users, including a flexible and scalable multi-threaded daemon, a command-line scanner, and an advanced tool for automatic database updates.	<a href="http://www.clamav.net/">http://www.clamav.net/</a>

<https://www.cisa.gov/free-cybersecurity-services-and-tools>



# NSA Cybersecurity Services



Protective DNS/  
Secure Web Gateway



Vulnerability Scanning  
and Mitigation



Threat Intelligence  
Collaboration

## Contact NSA DIB Defense



[CYBERCENTER.NSA.GOV](https://cybercenter.nsa.gov)

[@NSACYBER](https://twitter.com/NSACYBER)

[DIB\\_DEFENSE@CYBER.NSA.GOV](mailto:DIB_DEFENSE@CYBER.NSA.GOV)

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

 Kelley Kiernan

- ▼ DASHBOARD
- ACTIVITIES
- MEMBERS
- CYBER READINESS

CYBER READINESS CHECK RESULTS (800-171) ?

### NIST 800-171 Score



#### NIST 800-171 Score

NIST 800-171 provides agencies with recommended security requirements for protecting the confidentiality of CUI and applies to all components of nonfederal systems and organizations that process, store, and/or transmit CUI.

#### Actions

➤ [Return to NIST 800-171 Assessment](#)

#### History

No History available.

### CMMC Level 1 Score



#### CMMC Level 1 Score

### CMMC Level 2 Score



#### CMMC Level 2 Score

## NIST 800-171



#### Access Control

These questions ask about your policies to control access to your company's network systems.

1. Do you limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)?


➤ [More Info](#)

- Authorized users are identified.  Yes  No  Not Applicable  Answer Later
- Processes acting on behalf of authorized users are identified.  Yes  No  Not Applicable  Answer Later
- Devices (and other systems) authorized to connect to the system are identified.  Yes  No  Not Applicable  Answer Later
- System access is limited to authorized users.  Yes  No  Not Applicable  Answer Later
- System access is limited to processes acting on behalf of authorized users.  Yes  No  Not Applicable  Answer Later
- System access is limited to authorized devices (including other systems).  Yes  No  Not Applicable  Answer Later

# DON CISO'S BLUE CYBER

POWERED BY




Department of Defense  
Procurement Toolbox

[Home](#) [FAQs](#) [Calendar](#) [Contact Us](#)

Search

Government Furnished Property ▾
Unique ID ▾
eBusiness ▾
Purchase Card ▾
Cybersecurity ▾
Procure to Pay (P2P) ▾
Contract Closeout ▾
SAM.gov ▾

[Home](#) » [Cybersecurity](#) » [Other Resources](#)

Cybersecurity in DoD Acquisition Regulations

- Policy/Regulations
- FAQs
- Other Resources


## Other Resources


Name	Date	
One Pager: Safeguarding Covered Defense Information – The Basics	Current Version	<a href="#">View &gt;&gt;</a>
About the Cybersecurity Evaluation Tool (CSET) Tool	Current Version	<a href="#">View &gt;&gt;</a>
Briefing Slides from June 23, 2017 Public Meeting on Network Penetration Reporting and Contracting for Cloud Services	Current Version	<a href="#">View &gt;&gt;</a>
What Happens on December 31, 2017	Current Version	<a href="#">View &gt;&gt;</a>
Approach to Implementing NIST SP 800-171	Current Version	<a href="#">View &gt;&gt;</a>
Navigating Unclassified Information System Security Protections (1 of 2)	Current Version	<a href="#">View &gt;&gt;</a>
Script for Navigation Slides (2 of 2)	Current Version	<a href="#">View &gt;&gt;</a>
Webinars: Implementing DFARS Clause 252.204-7012 (Part 1)	Current Version	<a href="#">View &gt;&gt;</a>
Webinars: Implementing DFARS Clause 252.204-7012 (Part 2)	Current Version	<a href="#">View &gt;&gt;</a>
Webinars: Implementing DFARS Clause 252.204-7012 (Part 3)	Current Version	<a href="#">View &gt;&gt;</a>
To Assist in Development of the System Security Plan and Plans of Action	Current Version	<a href="#">View &gt;&gt;</a>
NIST MEP Handbook for NIST SP 800-171	Current Version	<a href="#">View &gt;&gt;</a>

# DON CISO'S BLUE CYBER

POWERED BY





[Login/Register](#)
[Contact Us](#)
[Search](#)


[About](#) - [Funding](#) - [Reports](#) - [Showcase](#) - [Announcements](#) - [Resources](#)

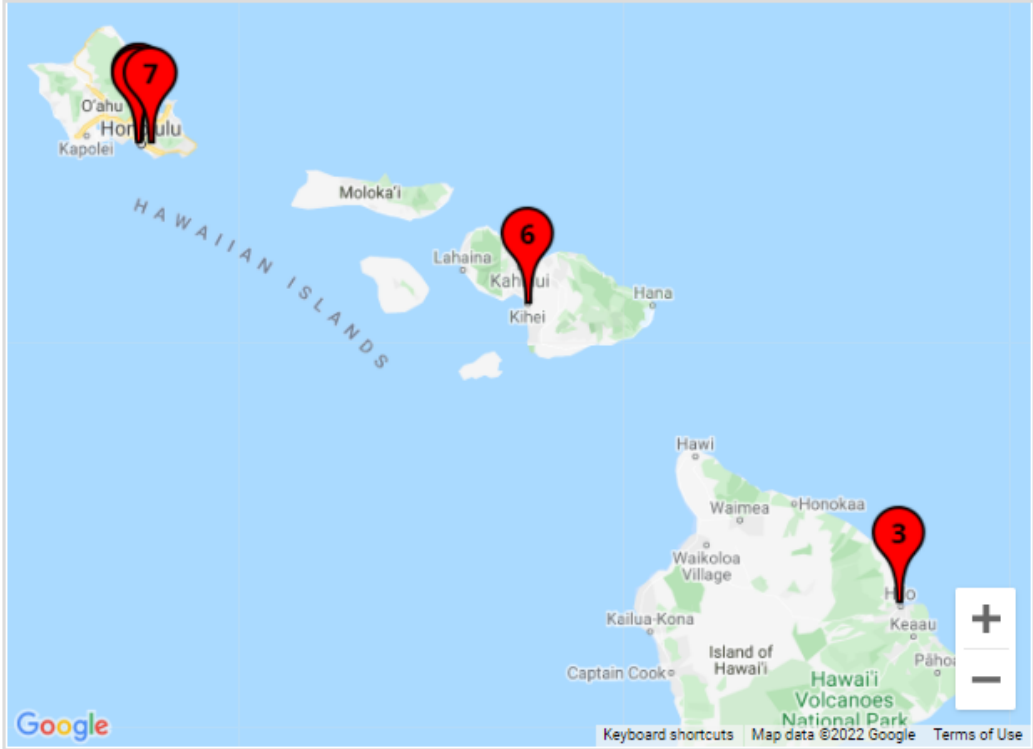
Home » Resources » Local Assistance » Hawaii

## 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](http://www.sbir.gov/local-assistance)

# DON CISO'S BLUE CYBER

POWERED BY



**FREE VIRTUAL EVENT**

# SBA CYBER SUMMIT

Experts offering practical, accessible and actionable resources to protect your business

**WEDNESDAY** | **TIME**  
**OCTOBER 26** | **NOON-5PM EDT**





[BIT.LY/SBACyberSummit](https://bit.ly/SBACyberSummit)



# SBA CYBER SUMMIT

**Executive Interview**

## Helping Small Business and Government Contractors Combat Cyber Attacks

Interview of Kelley Kiernan, Department of the Air Force and Space Force



**Kelley Kiernan**  
Dept of Air Force - Blue Cyber



**Jack Blenko**  
US SBA

**DATE** | **TIME**  
**OCT 26TH** | **3:30 - 4:00 PM EDT**

[BIT.LY/SBACyberSummit](https://bit.ly/SBACyberSummit)

All SBA programs and services are extended to the public on a nondiscriminatory basis.



Menu

POWERED BY



NEWS | Mar. 02, 2023

# Cohort Selected to Embark on New Innovations for National Security





# Daily, Open Office Hours

## Daily Event

### DAILY OFFICE HOURS

- Register here: [www.safcn.af.mil/CISO/small-business-cybersecurity-information/](http://www.safcn.af.mil/CISO/small-business-cybersecurity-information/)
- Nearly-daily opportunity to ask questions and get answers in-person.
- More information from [Kelley.Kiernan@us.af.mil](mailto:Kelley.Kiernan@us.af.mil)



# Every-Tuesday, Small Business Cybersecurity Ask-Me-Anything

## Weekly Event

**WEEKLY – Every Tuesday 1pm Eastern**

- Register here: [www.sbir.gov/events](http://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 [Kelley.Kiernan@us.af.mil](mailto:Kelley.Kiernan@us.af.mil)





# DAF CISO's Deep Blue Cyber Line-Up

Register on [www.sbir.gov/events](http://www.sbir.gov/events)

June 6 **“Where did these chips come from? - Cyber Supply Chain Risk Management”** The Blue Cyber Director, Kelley Kiernan will answer your cybersecurity questions and discuss the methods for understanding risk involved in the life-cycle of your hardware, IT and software being supplied to the government.

June 13 **“Basic Cyber Hygiene for your micro-Small Business”** A special 2-hour Session of Blue Cyber. The Blue Cyber Director, Kelley Kiernan and technical experts will cover the 15 security requirements in the FAR 52.204-21 (proposed CMMC Level 1) which comprise basic cyber hygiene for your small business.

June 20 **“So you want to bring IT/Software to the DoD? Working through the RMF/ ATO process”** Bring your questions and hear answers to demystify the process for Small Businesses to bring IT/Apps/SaaS/BOT/AI/ML into the DON/DAF/U.S. Army. Three experts will answer your questions about Risk Management Framework.

Jun 27 **“DON CISO's Blue Cyber “Cybersecurity Lollapalooza”** Ten agencies have services created to assist US Small Business with their journey to cybersecurity. These agencies have combined tens of thousands of dollars of free services to US Small Businesses and DoD suppliers.

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 ▼

JUN  
13  
2023

### Basic Cyber Hygiene for your micro-Small Business

**June 13, 2023 | 1:00pm to 3:00pm (ET)**

N/A

 Kelley Kiernan

 [kelly.s.kiernan@navy.mil](mailto:kelly.s.kiernan@navy.mil)

 [Visit Website](#)


**Webinar** **Navy**

JUN  
20  
2023

### So you want to bring IT/Software to the DoD? Working through the RMF/ ATO process

**June 20, 2023 | 1:00pm to 3:00pm (ET)**

N/A

 Kelley Kiernan

 [kelly.s.kiernan@navy.mil](mailto:kelly.s.kiernan@navy.mil)

 [Visit Website](#)


**Webinar** **Navy**

JUN  
27  
2023

### DON CISO's Blue Cyber "Cybersecurity Resources Lollapalooza": Ten Agencies offer their services to US Small Businesses

**June 27, 2023 | 12:00pm to 4:00pm (ET)**

N/A

 Kelley Kiernan

 [kelly.s.kiernan@navy.mil](mailto:kelly.s.kiernan@navy.mil)

 [Visit Website](#)

**In-Person Event** **DoD**

All our Events are on SBA's SBIR Event Site



## Department of the Navy Cybersecurity Boot Camp

### DON CISO's Blue Cyber

# Walk Through of all 110 Requirements of NIST SP 800-171 Eight-Hour Boot Camp **FREE** and **PUBLIC**

**Regularly**  
**"Big" Event**

**REGULARLY – Month x and x, 2023 11am to 3pm Eastern**

Register here: [www.sbir.gov/events](http://www.sbir.gov/events)

- We will talk about what is gained by implementing NIST SP 800-171, which is a component of the DFARS 252-204-7012, which is a requirement in the small business contract you sign today. This talk is to help the C-suite understand the requirements as you ensure robust cybersecurity for your company's intellectual property, your employee's PII, your financial data and the protection of sensitive government data.
- More information from [Kelley.Kiernan@us.af.mil](mailto:Kelley.Kiernan@us.af.mil)



# Air Force and Space Force Cybersecurity Boot Camp

## DON CISO Small Business – Academic/Research Contractor and Potential Contractors

Monthly “Big”  
Event

### MONTHLY

- Register here: [www.sbir.gov/events](http://www.sbir.gov/events)
- Join hundreds of your peers at the DON CISO's Cybersecurity Boot Camp. Come away having heard powerful speakers and learning what cybersecurity steps are necessary to protect your intellectual property and DoD Sensitive Data.
- More information from [Kelley.Kiernan@us.af.mil](mailto:Kelley.Kiernan@us.af.mil)



# Everybody Handles Federal Contracting Information!

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

### Monthly Event

**MONTHLY – June 13 1pm Eastern**

- Register here: [www.sbir.gov/events](http://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 [Kelley.Kiernan@us.af.mil](mailto:Kelley.Kiernan@us.af.mil)

## Blue Cyber Small Biz Cybersecurity Boot Camp

Sign-up at  
[www.sbir.gov/  
events](http://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](http://www.sbir.gov/events)
- 4. FORTY** short, ultra-relevant cybersecurity presentations/videos
- 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!**

POWERED BY





# Kelley Kiernan

## DON SBIR/STTR Program Office, Chief Technology Officer on Detail to the DON Chief Information Security Officer (CISO)

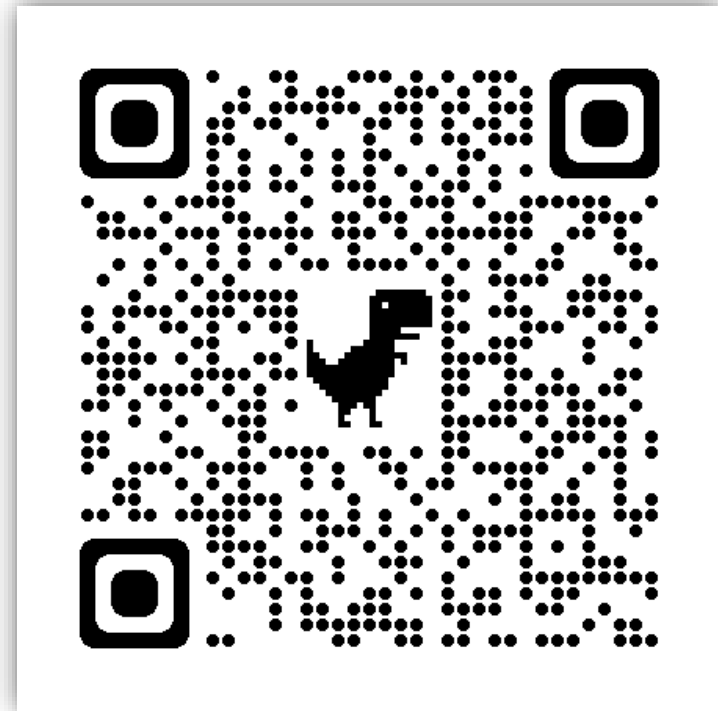
**STATEMENT OF LIMITATION OF AUTHORITY:** You are hereby notified that I do not have the authority to direct you in any way to alter your contractual obligations. Further, if the Department of the Navy, as the result of the information obtained from discussions or emails, does desire to alter your contract requirements, changes will be issued in writing and signed by the contracting officer. You should take no action on any change unless and until you receive such a contract modification.



## Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DON CISO Blue Cyber Educational Series and be found [here](#) !
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to [Kelley.Kiernan@us.af.mil](mailto:Kelley.Kiernan@us.af.mil)
  - **Daily** Office Hours for answering/researching **your** questions about DON Small Business cybersecurity and data protection!

**Every Tuesday**, 1pm Eastern, dial in for the DON CISO's Small Business Cybersecurity Ask-Me-Anything. Register at [www.sbir.gov/events](http://www.sbir.gov/events)





# DON CISO'S BLUE CYBER

POWERED BY



## 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!



### BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

[CYBERSECURITY BOOT CAMP for SMALL BUSINESS February 28, 10AM - 4PM EST LINK](#)



### EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING

[Click here for the registration link and agenda](#) for the Small Business Every-Tuesday Small Business Cybersecurity Ask-Me-Anything"

### BLUE CYBER EVENTS CALENDAR

Blue Cyber Events are all on [www.sbir.gov/events](http://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	+

### QUICK LINKS

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

The Blue Cyber Education Series for Small Businesses and Academic/ Research Institutions is in its second year and has made over 13K outreach contacts in the U.S. Small Business ecosystem since April 2021.

Blue Cyber is dedicated to an early-partnership with Defense Industrial Base small business contractors and potential contractors arm them with the latest in cybersecurity best practices.

**Every Day** there are FREE-PUBLIC office hours with SBIR/STTR and small business firms, to connect them to resources and answer their questions. Sign up for Open Office Hours [HERE](#)

**Every Tuesday** FREE-PUBLIC Cybersecurity Ask-Me-Anything webinars at 1pm Eastern;

**Every Month** A FREE-PUBLIC all-day boot camp

## Events

All FREE and PUBLIC  
[www.sbir.gov/events](http://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 SP8S 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	+