

AN OFFERING IN THE BLUE CYBER SERIES:

# Small Business Needs Big Cybersecurity

Version 5 Apr 2022

#9 in the Blue Cyber Education Series



# The slides are located at: [www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/](http://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/)

**DEPARTMENT OF AIR FORCE CISO'S BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS**

**DAF CISO'S BLUE CYBERSECURITY BOOT CAMP APRIL 20, 2022 | 10 AM-4PM EST LINK**

**DAF CISO'S EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING**

**BLUE CYBER EVENTS CALENDAR**

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

**Click here for the registration link and agenda** for the "DAF CISO's Every-Tuesday Small Business Cybersecurity Ask-Me-Anything"

The Air Force and Space Force Chief Information Security Officer has created the Blue Cyber Education Series for Small Businesses and Academic/Research Institutions. This program provides the following Small Business Cybersecurity Materials and an Every-Tuesday Cybersecurity Ask-Me-Anything.

The Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs allow small, high-tech U.S. businesses and academia the opportunity to provide innovative research and development solutions in response to critical U.S. Department of the Air Force needs. Find the main DAF SBIR/STTR page? [Find it here!](#)

The Department of the Air Force is dedicated to an early-partnership with Defense Industrial Base Small Businesses to arm them with the latest in cybersecurity best practices.

Need a quick-reference handout of available resources? [Find it here!](#)

Please direct any questions to [Kelley.Kiernan@us.af.mil](mailto:Kelley.Kiernan@us.af.mil)

**QUICK LINKS**

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

**SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS** +

**SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS** +

**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** +



# 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 Air Force Small Businesses

As small businesses drive innovation and support the Department of the Air Force (DAF) missions with cutting-edge technologies, it is vital we work together to protect DAF 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 DAF sensitive data and networks.

The DAF 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 DAF. 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 DAF Airmen and Guardians 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.





# 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 Systems

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

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

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

DFARS Clause  
252.204-7021  
Cybersecurity  
Maturity Model  
Certification  
Requirement



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

This DFARS is under review and it's status will not be known until late 2022 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/)



# So what has changed with CMMC 2.0?

A re-focus on the FAR and DFARS requirements.

- FAR Clause 252.204-21 still requires 15 security controls with no POAM. Law since 2013.

This is the proposed Foundational Level of CMMC 2.0

- DFARS Clause 252.204-7012 still requires 110 security controls implemented as the definition of adequate protection for DoD CUI. Law since 2017.

This is the proposed Advanced Level of CMMC 2.0

- CMMC 2.0 will become a contract requirement once rulemaking is completed. Late 2022 at the earliest.

DFARS Clause  
252.239-7010  
Cloud Computing  
Services

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

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

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

DFARS Clause  
252.204-7019/20  
NIST SP 800-171  
DoD Assessment  
Requirements.

DFARS Clause  
252.204-7021  
Cybersecurity  
Maturity Model  
Certification  
Requirement



## 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.



## Everybody Handles FCI!

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

**Friday, April 22, 1-3pm EDT**

- Register here: <https://www.zoomgov.com/meeting/register/vJlsduisqz4iHuEjsCpWOkcbJZF14FrT-8s>
- The Blue Cyber Director, Kelley Kiernan will cover the 17 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



## 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

# Welcome to the DIBNet portal

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

## Cyber Reports

[Report a Cyber Incident](#)

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

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

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

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

[FAR 52.204-25](#) Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

### Need Assistance?

Contact DoD Cyber Crime Center (DC3)

[DCISE@dc3.mil](mailto:DCISE@dc3.mil)

Hotline: (410) 981-0104

Toll Free: (877) 838-2174

## DoD's DIB Cybersecurity (CS) Program

[Apply Now!](#)

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

[DIB CS Participant Login](#)

[Voluntary Report](#)

### Cyber Threat Roundup

The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. For the latest edition of the Cyber Threat Roundup, please click [here](#).

For more information about other products, please apply to the [DIB CS Program](#).

### Need Assistance?

Contact the DIB CS Program Office

[OSD.DIBCSIA@mail.mil](mailto:OSD.DIBCSIA@mail.mil)

Hotline: (703) 604-3167

Toll Free: (855) DoD-IACS

Fax: (571) 372-5434

[https://  
dibnet.dod.mil](https://dibnet.dod.mil)

**A DoD-approved Medium Assurance Certificate is required to access DIBNet services. To obtain a DoD-approved Medium Assurance Certificate, please [click here](#).**

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2021-3218, 22 September 2021.



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

1 Apr 22

## Cyber Threat Roundup

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

### Contents

Articles.....	2
Nation-State Hackers Ramp Up Ukraine War-Themed Attacks.....	2
Satellite Modems Nexus of Worst Cyberattack of Ukraine War .....	2
Google TAG Details Cyber Activity With Regard to the Invasion of Ukraine .....	2
Hackers Target Russian Federal Air Transport Agency.....	2
Belarusian “Ghostwriter” Actor Picks Up BitB for Ukraine-Related Attacks .....	2
Viasat Confirms Satellite Modems Were Wiped with Acidrain Malware .....	3
Chinese Hacking Group Uses New Fire Chili Windows Rootkit.....	3
Lazarus Trojanized DeFi App for Delivering Malware .....	3
New Fatahrat Model: Purple Fox Hackers Are Increasing Their Botnet Infrastructure.....	3



# 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;

---

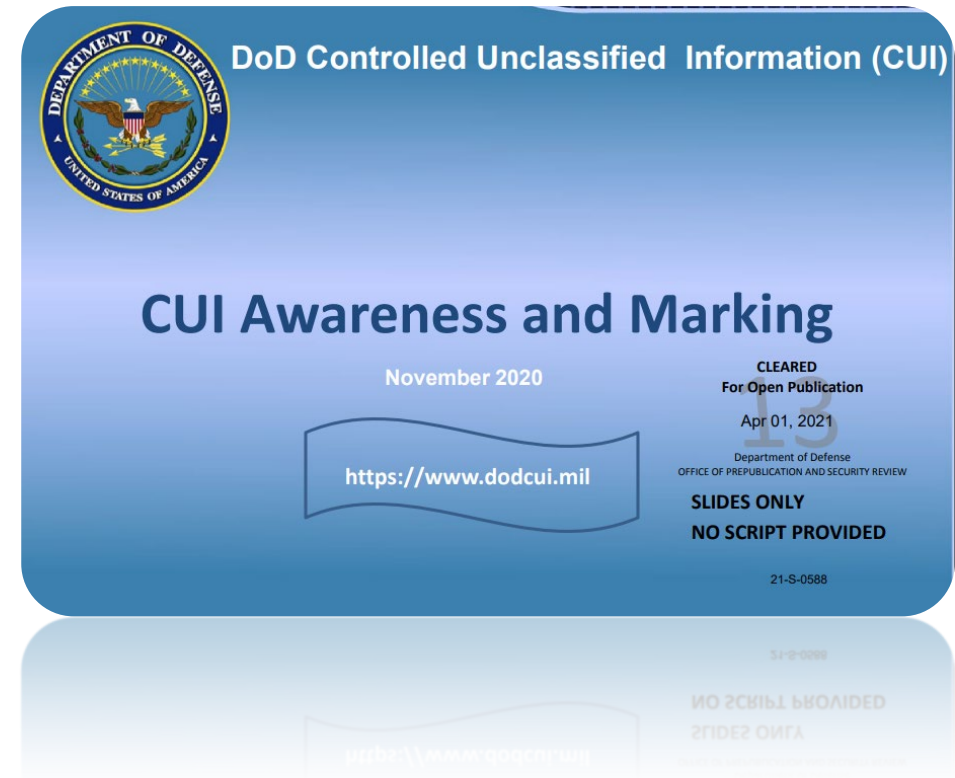
**OR** collected/developed/received/transmitted/used/ stored by the contractor in performance of contract.



# 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>







# 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 it's 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 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	



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



Self-Assessment



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



Flow the Requirement Down



Update your Self-Assessment



NIST SP 800-171



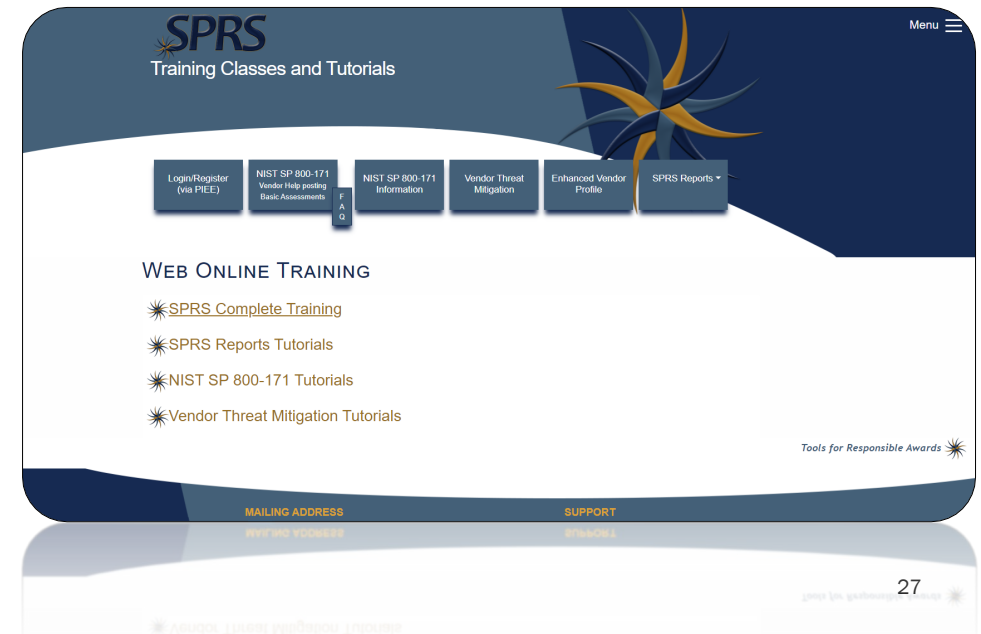
# How to enter a Basic Assessment Data into SPRS

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... Plan	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 NIST MEP Handbook

NIST Manufacturing Extension Partnership (MEP) Handbook will walk you through all 110 requirements and provide a list of process and policy documents you would create to have a robust CUI protection program

## 3.14.2 *Provide protection from malicious code at appropriate locations within organization information systems.*

Does the company employ malicious code protection mechanisms at system entry and exit points to minimize the presence of malicious code? System entry and exit points may include firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices.

Yes No Partially Does Not Apply Alternative Approach

Does the system automatically update malicious code protection mechanisms?

Yes No Partially Does Not Apply Alternative Approach

### Additional Information

Malicious code protection mechanisms (e.g., anti-virus, anti-malware and anti-spyware) include, for example, signature definitions, heuristics, and behavior analyzers. Due to information system integrity and availability concerns, companies should consider the methodology used to carry out automatic updates.

### Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code protection
- procedures addressing security alerts,

mechanisms

- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- test results from the installation of software and firmware updates to correct information system flaws installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system



# You Have Help with NIST SP 800-171A, Assessing Security Requirements for CUI


- The NIST SP 800-171A provides nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements.
- The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments.

3.14.2	<b>SECURITY REQUIREMENT</b> Provide protection from malicious code at designated locations within organizational systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	3.14.2[a] <i>designated locations for malicious code protection are identified.</i>
	3.14.2[b] <i>protection from malicious code at designated locations is provided.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine:</u> [SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system security plan; system configuration settings and associated documentation; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; scan results from malicious code protection mechanisms; system design documentation; system audit logs and records; other relevant documents or records]. <u>Interview:</u> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility]. <u>Test:</u> [SELECT FROM: Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting or implementing malicious code scanning and subsequent actions].



## New Documentation Guides

<https://www.acq.osd.mil/cmmc>

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

HomeAboutModelAssessmentsImplementationDocumentationResources

▼

**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 red added for emphasis

... (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 DAF 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 DAF 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 DAF is considering sharing with the contractor mission-essential?
- Is the CUI the DAF 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



# 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

**DoD SAFE** Logged on as user: *KIER...*

Home Drop-Off Request a Drop-Off Pick-up Outbox Help Logout

- + 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
  - 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 but only if solicited by CAC users.




# 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.





UNITED STATES AIR FORCE

# FAST TRACK AUTHORITY TO OPERATE (ATO)

**CIO  
INTENT:**

Provide an alternative pathway within the Risk Management Framework to grant an ATO which better manages cybersecurity risk by shortening timelines and shifting the focus from exhaustive documentation of controls to the assessment of demonstrable cybersecurity in an operationally relevant environment

## BACKGROUND

The Air Force ATO approval process under RMF to date has been very resource-intensive. While the ATO approval process is an important contributor to the critical tasks of implementing cybersecurity and managing the risk of information systems, delays in fielding new systems can bring their own risks by extending the use of legacy (often less secure) capabilities.

Therefore, in our implementation of RMF and the ATO process, we must balance between:

- (a) the valuable foundational work of identifying and understanding what we propose to introduce to the Air Force Information Network (AFIN); and
- (b) the need to modernize rapidly to keep pace with the ever-evolving technology and threat in the cyber domain.

On March 18, 2019, Air Force Deputy Chief Information Officer signed a memo adding “**Fast Track ATO**” as a pathway within AF Risk Management Framework to obtain an ATO.

On March 22, 2019, Air Force Undersecretary signed a memo giving Authorizing Officials (AOs) the discretion to make an authorization decision based on a combination of the system meeting a cybersecurity baseline, conducting risk-based assessments and a continuous monitoring strategy.

The Fast Track Authorization to Operate (ATO) allows the AO to make an authorization decision based on the review of

- a Cybersecurity Baseline,
- a Threat-Risk Assessment (e.g. penetration test), and
- an Information System Continuous Monitoring Strategy.



# 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

Fast Track accelerates RMF steps “**Select**” through “**Authorize**” by focusing on operationally relevant risk identification, and ensuring threat-informed risk assessments for DAF systems and missions. The objective being the integration of the Acquisition, Test, and Operations communities in assessing and determining system and mission risk to better inform mission owners.

Additionally, Fast Track ATO is for managing risk for the life-cycle of a system; not a one and done. **The job does not end when the ATO is issued, it only begins...**



# Do I need an AT0?

# Maybe not...

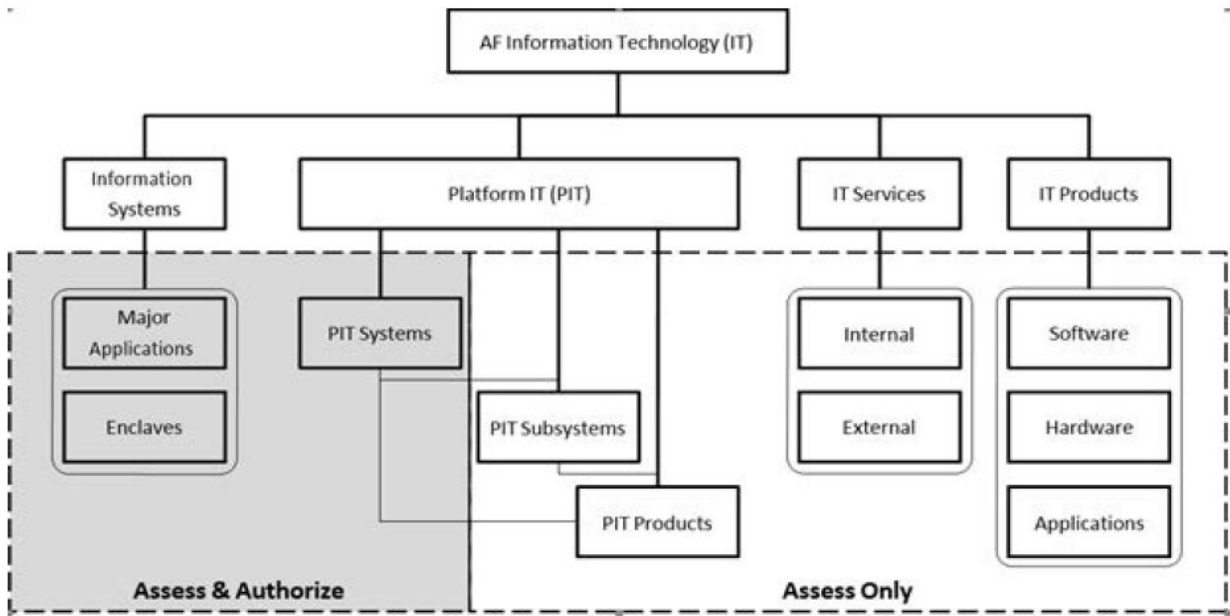


Figure 1: DAF Information Technology (IT)  
Reference: AFI 17-101, Fig.1.1. DAF IT Categories

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.





Enter Terms

SEARCH



# 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 ▶

SBIR/STTR Firms!

## 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



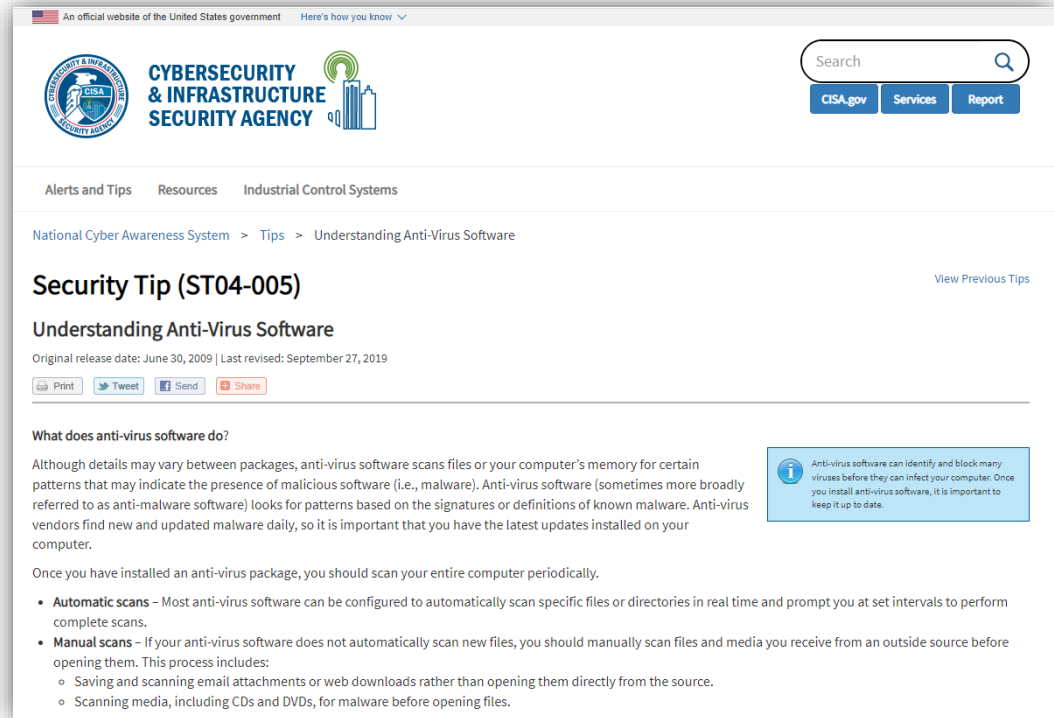




# When it's time to get strong anti-virus



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



[www.cisa.gov/uscert/ncas/tips/ST04-005](https://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
Immunet Antivirus	Basic	Cisco	Immunet is a malware and antivirus protection system for Microsoft Windows that utilizes cloud computing to provide enhanced community-based security.	<a href="https://www.immunet.com/">https://www.immunet.com/</a>
Microsoft Defender Antivirus	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]) antivirus 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>



nsa.gov/About/Cybersecurity-Collaboration-Center/PDNS/

Cyber Leadership T... SAF/CNZ - Blue Cy... AQR AMA Reg Link Boot Camp Registra...

Other bookmarks

NSA/CSS

About Press Room Careers History

# Protective Domain Name System Services

Drive Down Risk | Protect DOD Information

**CONTACT FORM**



# 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)

[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>



www.sbir.gov/local-assistance



Login/Register

Contact Us

Search



About

Funding

Reports

Showcase

Announcements

Resources

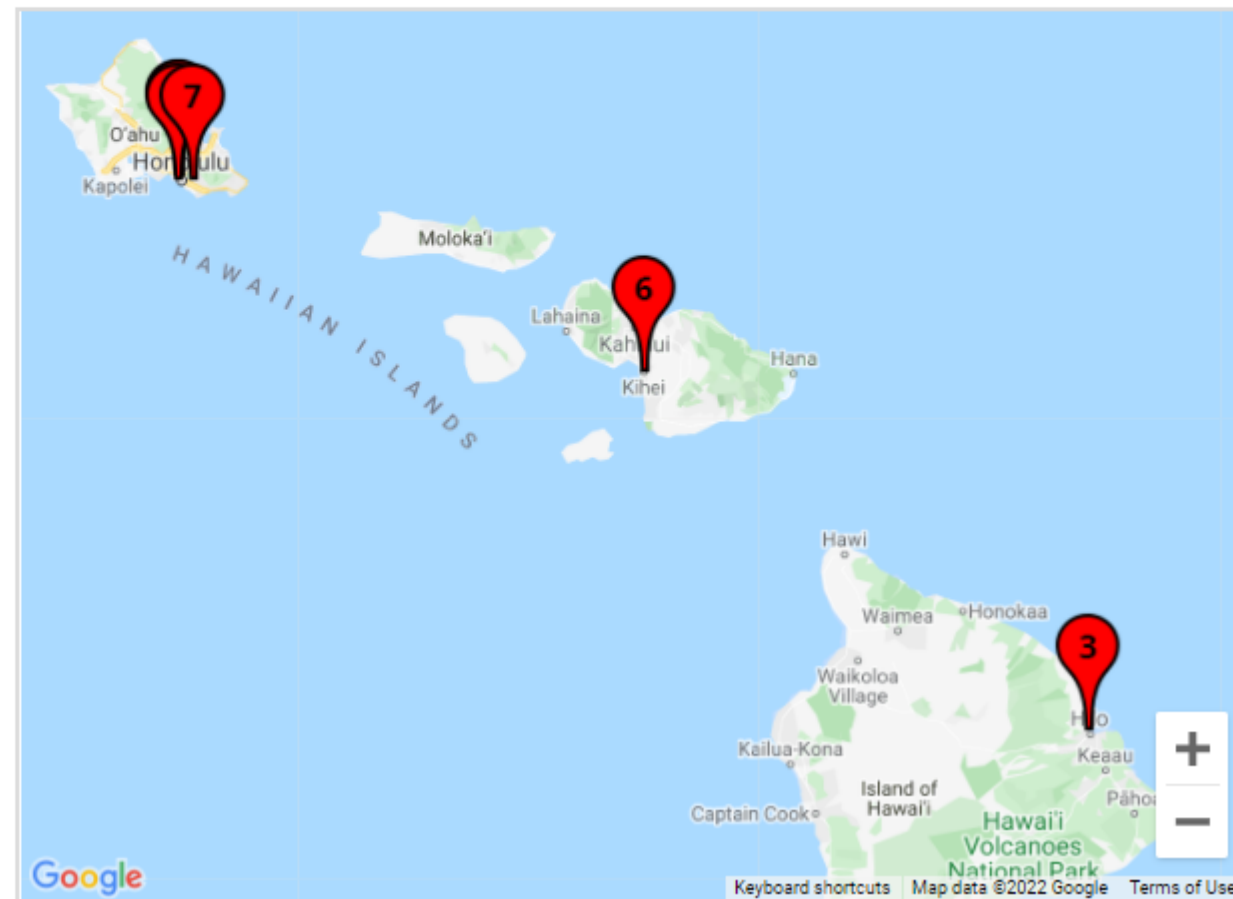
Home » Resources » Local Assistance » Hawaii

## 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





The Blue Cyber Education Series for DAF Small Businesses on the DAF CISO webpage  
[www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/](http://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/)

**Daily Office Hours** for answering/researching **your** questions about DAF Small Business cybersecurity and data protection!

**Every Tuesday 1pm EST**, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar:

[https://www.zoomgov.com/webinar/register/WN\\_6Gz84TQGRvm6YHMSVyEOQg](https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVyEOQg)

## DEPARTMENT OF AIR FORCE CISO'S BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

DAF CISO'S BLUE CYBERSECURITY BOOT CAMP APRIL 20, 2022 | 10 AM-4PM EST [LINK](#)



### DAF CISO'S EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING

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

The Air Force and Space Force Chief Information Security Officer created the Blue Cyber Education Series for Small Businesses and Academic/Research Institutions. This program provides the following Small Business Cybersecurity Materials and an Every-Tuesday Cybersecurity Ask-Me-Anything.

The Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs allow small, high-

### BLUE CYBER EVENTS CALENDAR

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

#### SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS

- FOLLOWING THE CYBERSECURITY DFARS IN YOUR SMALL BUSINESS CONTRACT
- DOD CYBERSECURITY INCIDENT REPORTING
- GET YOUR SPRS ON! DOCUMENTING COMPLIANCE WITH NIST SP 800-171
- CAN I GIVE MY CONTRACTOR CUI?
- FAST TRACK ATO AND DAF AUTHORIZATION TO OPERATE PRIMER
- PROTECTION OF COMMON TYPES OF DOD CONTROLLED UNCLASSIFIED INFORMATION
- DOD CLOUD COMPUTING

#### 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





## AGENDA

Eastern Standard Time

**1000**

Welcome: Air Force and Space Force Chief Information Security Officer, Mr. Aaron Bishop [Bio Link](#)

**1015**

"FAR and DFARS in your Small Business Contract" and "Get Your SPRS On," Kelley Kiernan [Bio Link](#)

**1030**

DoD Cyber Crime Center, DoD Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) video "Unclassified Threat Briefing for Small Businesses"

**1100**

"Common Types of DOD CUI" and "Can I give my Contractor CUI?" Kelley Kiernan

**1130**

"Where to begin with NIST SP 800-171" and "Questions to ask a cybersecurity provider" Kelley Kiernan

**1200**

Defense Contract Management Agency video "Encryption Requirements for NIST SP 800-171"

**1230**

"The Small Business Cybersecurity Ecosystem" Ms. Eileen Sánchez, Chief, Defense Industry Cybersecurity Resilience and Innovation Program Director, California Advanced Supply Chain Analysis & Diversification Effort (CASCADE), Military Affairs, California

April Event

## PUBLIC EVENT

# DAF CISO'S BLUE CYBER BOOT CAMP: CYBERSECURITY FOR SMALL BUSINESSES

APRIL 20, 2022 | 10 AM-4PM EST

# JOIN US!

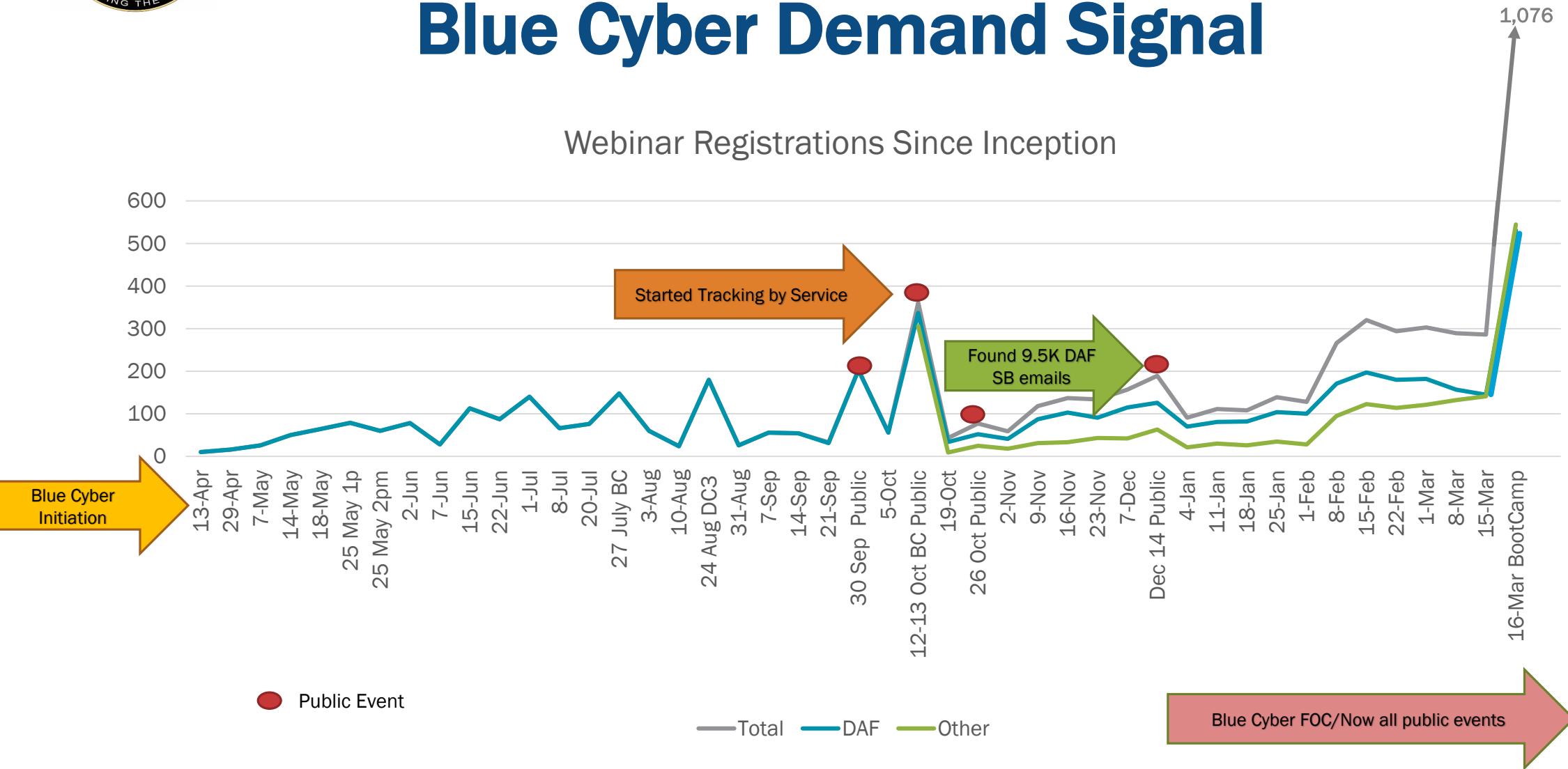
Join us for the first-ever Air Force and Space Force Chief Information Security Officer's Blue Cyber Small Business Cybersecurity Boot Camp.

**FREE**, All-Day information sessions Small Business Cybersecurity boot camp. Join hundreds of your peers and learn about the resources available to you to help secure your small business and to comply with the DoD's requirements for small business contractors. Hear from Mr. Aaron Bishop, the DAF CISO about the imperative for small businesses to protect their data and networks, as well as protecting sensitive DOD data. Also, hear all



# Blue Cyber Demand Signal

Webinar Registrations Since Inception







# **Kelley Kiernan**

## **DAF SBIR/STTR Program Office, Chief Technology Officer on Detail to the DAF 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 Air Force, 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.



# **Wednesday, April 20 10am to 4pm EST**

## **Free Cybersecurity Boot Camp for Small Businesses**

- Register here: <https://www.afsbirsttr.af.mil/Portals/60/documents/BlueCyber-DAF-BootCamp%2020%20April%2022.pdf>
- Free modules to take you from the DFARS in your contract through implementing NIST SP 800-171
  - Come away with actionable information
  - Understand the requirements and be better able to estimate your costs
  - Finish the day with resources you can turn to for help with your cybersecurity journey
  - Invite your ecosystem! Share LinkedIn posts from Kelley Kiernan or USAF SBIR/STTR
  - This was created for our DIB small businesses! See you there!

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**

### **Friday, April 22, 1-3pm EDT**

- Register here: <https://www.zoomgov.com/meeting/register/vJlsduisqz4iHuEjsCpWOkcbJZF14FrT-8s>
- The Blue Cyber Director, Kelley Kiernan will cover the 17 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



# Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage:  
<https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/>
- 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 DAF Small Business cybersecurity and data protection!

**Every Tuesday at 1pm EST**, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar:

[https://www.zoomgov.com/webinar/register/WN\\_6Gz84TQGRvm6YHMSVyE0Qg](https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVyE0Qg)