

AN OFFERING IN THE BLUE CYBER SERIES

Basic Cyber Hygiene FAR 52.204-21 The Proposed CMMC Level 1



AFWERX

VERSION: October 2023

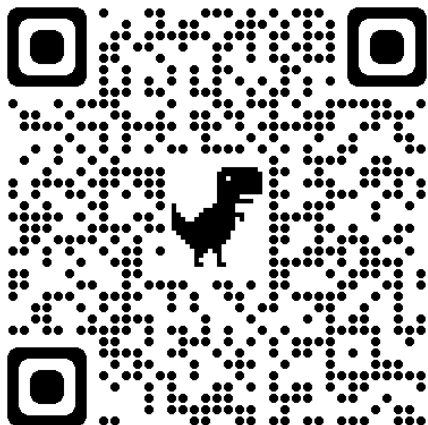
#16 IN THE DAF CISO's BLUE CYBER EDUCATION
SERIES

Website

The Blue Cyber Education Series for Small Businesses [webpage](#)

Daily Office Hours

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



DAF/CN OFFICE OF THE CHIEF INFORMATION OFFICER
ABOUT US
BIOGRAPHIES
CYBERSECURITY
CONTACT US

BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

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

CLICK BELOW FOR VIDEOS

CLICK BELOW FOR PRESENTATIONS

CLICK BELOW 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"

SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS

SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS

SMALL BUSINESS CYBERSECURITY MEMOS

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

BLUE CYBER EVENTS CALENDAR

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

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

QUICK LINKS

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

Events

All FREE and PUBLIC
[www.sbir.gov/events](#)

40Presentations

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
DOO 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 DOO CUI
SMALL BUSINESS CYBERSECURITY RESOURCES
SMALL BUSINESS NEEDS BIG CYBERSECURITY
THREAT BRIEFING FOR SMALL BUSINESSES
WHERE TO BEGIN WITH NIST SP 800-171
DOO CLOUD COMPUTING
HACKERS ARE WATCHING YOU
HARDENING WINDOWS FOR NIST SP 800-171
QUESTIONS TO ASK WHEN CHOOSING A CYBERSECURITY SERVICES
DEMISTIFYING 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
DOO MENTOR-PROTEGE PROGRAM

SMALL BUSINESS CYBERSECURITY MEMOS

Poll



**How many employees
do you have in your
small business or
academic/research
institution?**

The slides are located at: www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/

DAF CISO'S BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

31 OCTOBER CYBERSECURITY BOOTCAMP for SMALL BUSEINESS register [HERE](#)

CLICK BELOW FOR VIDEOS

CLICK BELOW FOR PRESENTATIONS

CLICK BELOW FOR MEMOS

CLICK FOR EVENTS

EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING WEBINAR

DAF CISO'S BLUE CYBER EVENTS CALENDAR

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

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

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

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

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

FOLLOWING THE CYBERSECURITY DFARS IN YOUR SMALL BUSINESS

DOD CYBERSECURITY INCIDENT REPORTING

GET YOUR SPRS ON! DOCUMENTING COMPLIANCE WITH NIST SP 800-171

CAN I GIVE MY CONTRACTOR CUI?

DAF FAST TRACK ATO INFORMATION

PROTECTING OF COMMON TYPES OF DOD CUI

SMALL BUSINESS CYBERSECURITY RESOURCES

SMALL BUSINESS NEEDS BIG CYBERSECURITY

THREAT BRIEFING FOR SMALL BUSINESSES

WHERE TO BEGIN WITH NIST SP 800-171

DOD CLOUD COMPUTING

HACKERS ARE WATCHING YOU

HARDENING WINDOWS FOR NIST SP 800-171

QUESTIONS TO ASK WHEN CHOOSING A CYBERSECURITY SERVICES

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

SECURING THE DEFENSE INDUSTRIAL BASE

CISA TO THE RESCUE! CISA RESOURCES

COST EFFECTIVE CYBERSECURITY BY DAU PROF PAUL SHAW

17 WAYS TO BE MORE CYBER SECURE TODAY!

SMALL BUSINESS CYBERSECURITY MEMOS

Kelley Kiernan
DAF CISO's Blue Cyber Initiative Director

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 DAF, 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.

NIST 800-171 SECURITY REQUIREMENTS

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

Administrative (e.g., policies, standards & procedures)

Technical Configurations (e.g., security settings)

Software Solution

Hardware Solution

Software or Hardware Solution

Assigned Tasks To Cybersecurity Personnel

Assigned Tasks To IT Personnel

Assigned Tasks To Application/Asset/Process Owner

Configuration or Software Solution

Configuration or Software or Hardware or Outsourced Solution

NIST 800-171 SECURITY REQUIREMENTS

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1				3.5.1					3.10.1			3.13.1	3.14.1
3.1.2				3.5.2									3.14.2
							3.8.3		3.10.3				
									3.10.4				3.14.4
3.1.20									3.10.5			3.13.5	3.14.5
3.1.22													

17 NIST SP 800-171 Security Requirements are the same as:
 CMMC 2.0 Level 1 Security Requirements and the same as
 FAR 52.204-21 Security Requirements

Same/Same/Same

DoD CIO's Definition of FCI

Information, not intended for public release,

that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government,

but not including information provided by the Government to the public (such as on public websites)

or simple transactional information, such as necessary to process payments

WHAT IS THE DIFFERENCE BETWEEN Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)?

FCI is information not intended for public release.

FCI is provided by or generated for the Federal Government under a contract to develop or deliver a product or service.

CUI and FCI share important similarities and a particularly important distinction. Both CUI and FCI include information created or collected by or for the Government, as well as information received from the Government.

However, while FCI is any information that is “not intended for public release,” CUI is information that requires safeguarding and may also be subject to dissemination controls.

**Information that is collected, created, or received
pursuant to a government contract**

FCI

Information that is not marked as
public or for public release.

**Minimum Cybersecurity Requirements
in a non-federal information system:**

Basic Safeguarding Clause: 48 CFR §
52.204-21*

CUI

Information that is marked or
identified as requiring
protection under the CUI
program.

**Minimum Security
Requirements in a non-federal
information system:**
NIST SP 800-171

**Public
Information**

Public information or information
marked for public release.

**Minimum Security Requirements
in a non-federal information
system: None**

*also excludes simple transactional information.

<https://isoo.blogs.archives.gov/2020/06/19/%E2%80%8Bfci-and-cui-what-is-the-difference/>

Does your contract handle CUI?

FIND OUT!

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting is in ALL DAF contracts, so its presence is not the answer

Ask your contracting Officer

AN OFFERING IN THE BLUE CYBER SERIES

Check out this video
on the Blue Cyber webpage

VIDEO

Protection of Common Types of DOD CUI



VERSION 14 MARCH 2022

#6 in the BLUE CYBER EDUCATION SERIES



AN OFFERING IN THE BLUE CYBER SERIES

Check out this lesson
on the Blue Cyber webpage

DOD INSTRUCTION 5230.24 “DISTRIBUTION STATEMENTS ON DOD TECHNICAL INFORMATION” a SBIR/STTR Contractor’s User Guide



VERSION: May 2023

#41 IN THE BLUE CYBER EDUCATION SERIES



17 Controls - Assess and Document

Access Control (AC)	9
AC.L1-3.1.1 – Authorized Access Control	9
AC.L1-3.1.2 – Transaction & Function Control	12
AC.L1-3.1.20 – External Connections	14
AC.L1-3.1.22 – Control Public Information	17
Identification and Authentication (IA)	19
IA.L1-3.5.1 – Identification	19
IA.L1-3.5.2 – Authentication	21
Media Protection (MP)	24
MP.L1-3.8.3 – Media Disposal	24
Physical Protection (PE)	26
PE.L1-3.10.1 – Limit Physical Access	26
PE.L1-3.10.3 – Escort Visitors	28
PE.L1-3.10.4 – Physical Access Logs	30
PE.L1-3.10.5 – Manage Physical Access	32
System and Communications Protection (SC)	34
SC.L1-3.13.1 – Boundary Protection	34
SC.L1-3.13.5 – Public-Access System Separation	37
System and Information Integrity (SI)	39
SI.L1-3.14.1 – Flaw Remediation	39
SI.L1-3.14.2 – Malicious Code Protection	42
SI.L1-3.14.4 – Update Malicious Code Protection	45
SI.L1-3.14.5 – System & File Scanning	47

Priority

Eleven of the Controls are considered 5-point risk (high risk) by the DOD.

DOD NIST SP 800-171 Assessment Methodology

<https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf>

Access Control (AC)	9
5 AC.L1-3.1.1 – Authorized Access Control	9
5 AC.L1-3.1.2 – Transaction & Function Control	12
AC.L1-3.1.20 – External Connections	14
AC.L1-3.1.22 – Control Public Information	17
Identification and Authentication (IA)	19
5 IA.L1-3.5.1 – Identification	19
5 IA.L1-3.5.2 – Authentication	21
Media Protection (MP)	24
5 MP.L1-3.8.3 – Media Disposal	24
Physical Protection (PE)	26
5 PE.L1-3.10.1 – Limit Physical Access	26
PE.L1-3.10.3 – Escort Visitors	28
PE.L1-3.10.4 – Physical Access Logs	30
PE.L1-3.10.5 – Manage Physical Access	32
System and Communications Protection (SC)	34
5 SC.L1-3.13.1 – Boundary Protection	34
5 SC.L1-3.13.5 – Public-Access System Separation	37
System and Information Integrity (SI)	39
5 SI.L1-3.14.1 – Flaw Remediation	39
5 SI.L1-3.14.2 – Malicious Code Protection	42
5 SI.L1-3.14.4 – Update Malicious Code Protection	45
SI.L1-3.14.5 – System & File Scanning	47

FAR 21 Requirement	NIST SP 800-171 Equivalent Requirement	NIST SP 800-171 Language
(b)(1)(i)	3.1.1 Technical Control	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).
(b)(1)(ii)	3.1.2 Technical Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(b)(1)(iii)	3.1.20 Technical Control Administrative Control	Verify and control/limit connections to and use of external information systems.
(b)(1)(iv)	3.1.22 Administrative Control	Control information posted or processed on publicly accessible information systems.
(b)(1)(v)	3.5.1 Technical Control	Identify information system users, processes acting on behalf of users or devices.

* One solution, could be others.

FAR 21 Requirement	NIST SP 800-171 Equivalent Requirement	NIST SP 800-171 Language
(b)(1)(vi)	3.5.2 Technical Control	Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.
(b)(1)(vii)	3.8.3 Configuration or Software or Hardware or Outsource	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.
(b)(1)(viii)	3.10.1 Administrative Control	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.
(b)(1)(ix)	3.10.3 Administrative Control	Escort visitors and monitor visitor activity.
(b)(1)(ix)	3.10.4 Administrative Control	Maintain audit logs of physical access.

** One solution, could be others.*

FAR 21 Requirement	NIST SP 800-171 Equivalent Requirement	NIST SP 800-171 Language
(b)(1)(ix)	3.10.5 Administrative Control Physical Control	Control and manage physical access devices.
(b)(1)(x)	3.13.1 Hardware Solution*	Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(b)(1)(xi)	3.13.5 Technical Control	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(b)(1)(xii)	3.14.1 Administrative Control	Identify, report and correct information and information system flaws in a timely manner.
(b)(1)(xiii)	3.14.2 Software Solution*	Provide protection from malicious code at appropriate locations within organizational information systems.
(b)(1)(xiv)	3.14.4 Technical Control	Update malicious code protection mechanisms when new releases are available.
(b)(1)(xv)	3.14.5 Software Solution*	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.

* One solution, could be others.

Laundry List of Artifacts which are meant to give you ideas of what kind of Objective Proof you can supply on each of the 110 requirements

- Documented policies, standards & procedures
- Supporting documentation to demonstrate how (software, hardware, etc.) is properly & securely implemented
- Screen shot of everything that could provide objective proof
- Documents or screenshot which demonstrate a capability
- Documents or screenshot to show how software or hardware are properly and securely configured
- Screen Shots groups and membership assignment
- Documentation to demonstrate change management practices reviewed/approved
- Data Flow Diagram (DFD)
- Screen shot of firewall rules with business justification
- Documentation of role-based security training being performed
- Screen shot of access control settings
- Screen shot of AD settings, or other IAM interface

Unofficial ! – Helpful Terms

- **Define - Policy/SOP/TTP**
- **Employ - Doing Something, Proof (audit log, email traffic, etc.)**
- **Maintain - Doing Something, Upkeep employ**
- **Establish - Procedure**
- **Implement - Doing Something, putting policy in place**
- **Document - Policy/SOP/TTP**
- **Authorize - Signed Policy/SOP/TTP/ATO/Risk Acceptance**
- **Report - Proof of doing something**
- **Protects - Doing Something/Implementation**
- **Configure - Doing Something**
- **Reviews - Proof of doing something**
- **Requires - Standards, Policy/SOP/TTP, validating that you are doing something**
- **Identify - Define (could be different ways to identify, document, interview, test),**

Both documents
are necessary



The screenshot shows the official website of the Chief Information Officer, U.S. Department of Defense. At the top left is the Department of Defense seal. To its right is the title "CHIEF INFORMATION OFFICER" and "U.S. DEPARTMENT OF DEFENSE". A search bar labeled "Search Chief Information" is in the top right. A dark blue navigation bar contains links: HOME, ABOUT DOD CIO, IN THE NEWS, LIBRARY, CYBER WORKFORCE, CMMC, and CONTACT US. A prominent yellow banner with red text reads: "UPDATES TO THE CMMC WEBSITE WILL BE LIMITED DURING THE CMMC 2.0 RULEMAKING PROCESS". Below this, the "CMMC DOCUMENTATION" section is highlighted with a blue bar. It contains three sub-sections: "Model Overview" with links to the Model Overview, CMMC 2.0 Spreadsheet and Mapping, and CMMC Glossary; "Scoping Guidance" with links to CMMC Level 1 and Level 2 Scoping Guidance; and "Assessment Guides" with links to CMMC Level 1, 2, and 3 Self-Assessment Guides. Two green arrows point to the "Scoping Guidance" and "Assessment Guides" sections. At the bottom, the URL "www.dodcio.defense.gov/CMMC/" is displayed in large red text.

CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE

HOME ABOUT DOD CIO IN THE NEWS LIBRARY CYBER WORKFORCE CMMC CONTACT US

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

CMMC DOCUMENTATION

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](#)

www.dodcio.defense.gov/CMMC/

How to use these CMMC 2.0 Documents

- Inventory your Information System
 - See the Blue Cyber “Where to begin with NIST SP 800-171”
- Scope your Assessment
- Utilize the Key Sections of the Self-Assessment Guide
 1. Assessment Objectives from NIST SP 800-171A
 2. Potential Assessment Methods
 3. Discussion (provides a practical understanding)
 4. Further Discussion
 5. Example
 6. Potential Assessment Considerations

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

- [a] the types of transactions and functions that authorized users are permitted to execute are defined; and
- [b] system access is limited to the defined types of transactions and functions for authorized users.

So 3.1.2 is not
one requirement
- it's two
requirements!

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

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

Examine

[SELECT FROM: Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing access control policy].

“Select from”....
not necessarily all

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

DISCUSSION [NIST SP 800-171 R2]

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of -origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

FURTHER DISCUSSION

Limit users to only the information systems, roles, or applications they are permitted to use and are needed for their roles and responsibilities. Limit access to applications and data based on the authorized users' roles and responsibilities. Common types of functions a user can be assigned are create, read, update, and delete.

Example

You supervise the team that manages DoD contracts for your company. Members of your team need to access the contract information to perform their work properly. Because some of that data contains FCI, you work with IT to set up your group's systems so that users can be assigned access based on their specific roles [a]. Each role limits whether an employee has read-access or create/read/delete/update -access [b]. Implementing this access control restricts access to FCI information unless specifically authorized.

This is the
simple
statement

Example: AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Potential Assessment Considerations

- Are access control lists used to limit access to applications and data based on role and/or identity [a]?⁵
- Is access for authorized users restricted to those parts of the system they are explicitly permitted to use (e.g., a person who only performs word-processing cannot access developer tools) [b]?⁶

Now Repeat, for each of the 17 Security Requirements

- Document your results
- Document your Artifacts
- Set a schedule to update
- Ask your questions

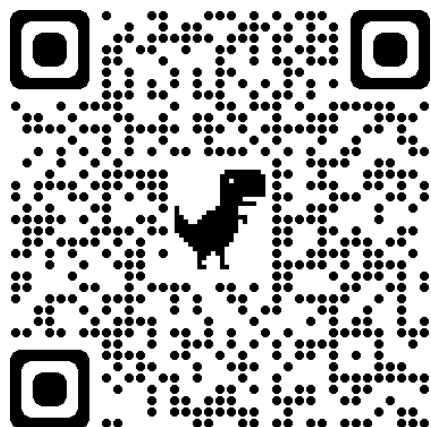
Access Control (AC)	9
AC.L1-3.1.1 – Authorized Access Control	9
AC.L1-3.1.2 – Transaction & Function Control	12
AC.L1-3.1.20 – External Connections	14
AC.L1-3.1.22 – Control Public Information	17
Identification and Authentication (IA)	19
IA.L1-3.5.1 – Identification	19
IA.L1-3.5.2 – Authentication	21
Media Protection (MP)	24
MP.L1-3.8.3 – Media Disposal	24
Physical Protection (PE)	26
PE.L1-3.10.1 – Limit Physical Access	26
PE.L1-3.10.3 – Escort Visitors	28
PE.L1-3.10.4 – Physical Access Logs	30
PE.L1-3.10.5 – Manage Physical Access	32
System and Communications Protection (SC)	34
SC.L1-3.13.1 – Boundary Protection	34
SC.L1-3.13.5 – Public-Access System Separation	37
System and Information Integrity (SI)	39
SI.L1-3.14.1 – Flaw Remediation	39
SI.L1-3.14.2 – Malicious Code Protection	42
SI.L1-3.14.4 – Update Malicious Code Protection	45
SI.L1-3.14.5 – System & File Scanning	47

Website

The Blue Cyber Education Series for Small Businesses [webpage](#)

Daily Office Hours

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



Events

All FREE and PUBLIC
www.sbir.gov/events

40 Presentations Vides and PowerPoints

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

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

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

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 DON, 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.

Daily, Open Office Hours

Daily
Event

DAILY OFFICE HOURS

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

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

Weekly
Event

WEEKLY – Every Tuesday 1pm Eastern

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

DAF CISO's Deep Blue Cyber Line-Up

Register on www.sbir.gov/events

October 3 “DIBCAC presents: An Encryption Primer and the Encryption requirements in NIST SP 800-171”

Listen to the Defense Contracting Management Agency's DIBCAC Team is talking with you about Encryption Requirements in NIST SP 800-171. The DCMA DIBCAC Team is the DOD's premier experts on contractor cybersecurity programs and they have helped hundreds of contractors improve their cybersecurity posture. The DIBCAC is the definitive source on DOD cybersecurity requirements.

October 10 “CISA to the Rescue” Join us to learn about services, free tools and resources for your SMB from the Cybersecurity Infrastructure Security Agency (CISA). JD Henry is part of a team of 52 national risk advisors at CISA. They will bring you actionable information on services and resources that are available for small businesses to augment their cybersecurity posture and improve their operational resiliency.

October 17 “Protect your Small Business: Basic Cyber Hygiene FAR 52-204-21 and the Proposed CMMC Level 1

A special 2-hour Session of Blue Cyber. The Blue Cyber Director, Kelley Kiernan and technical experts will cover the 17 security requirements in the FAR 52.204-21 which comprise basic cyber hygiene for any small business. The target audience is small businesses of any type, with or without government contracts. Every small business is welcome.

October 24 “Where did these Chips Come From: Supply Chain Risk Management for your Small Business” 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.

October 31 October Boot Camp - Protect Yourself From Ransomware!

[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

OCT
03
2023


Understand Encryption Today for your small business: DIBCAC presents: An Encryption Primer and the Encryption requirements in NIST SP 800-171

October 3, 2023 | 1:00pm to 3:00pm (ET)

N/A

 Kelley Kiernan

 kelly.kiernan@us.af.mil

 [Visit Website](#)

Webinar

Navy

OCT
10
2023


CISA to the Rescue!

October 10, 2023 | 1:00pm to 3:00pm (ET)

N/A

 Kelley Kiernan

 kelly.kiernan@us.af.mil

 [Visit Website](#)

Webinar

Navy

OCT
17
2023


“Protect your Small Business: Basic Cyber Hygiene FAR 52-204-21 and the Proposed CMMC Level 1” Cohosted with the University of Missouri AFEX Accelerator

October 17, 2023 | 1:00pm to 3:00pm (ET)

N/A

 Kelley Kiernan

 kelly.kiernan@us.af.mil

 [Visit Website](#)

Webinar

Navy

All our Events are on
SBA's SBIR
Event Site
www.sbir.gov/events

Blue Cyber Cybersecurity Boot Camp

Free and Open to the Public

Small Business Contractors, Academic/Research Contractors and Potential Contractors

Monthly “Big”
Event

TBD Monthly

12pm – 3pm Eastern

- Register here: 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 at <https://www.safcn.af.mil/Contact-Us/>

Everybody Handles Federal Contracting Information!

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

Monthly
Event

MONTHLY – TBD

1pm Eastern

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

Poll



**I have professional
cybersecurity help for
my small business.**

Blue Cyber Small Biz

Always Free
Always Public

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
- 4. FORTY** short, ultra-relevant cybersecurity presentations/videos
- 5.** Blue Cyber refers DoD Small Businesses to state/federal cyber resources

BLUE CYBER INITIATIVE

DON CISO'S BLUE CYBER SERIES

CYBERSECURITY FOR SMALL BUSINESSES

DAILY | WEEKLY | MONTHLY

JOIN US!

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

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

JOIN US!

DAF CISO's Blue Cyber

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

AFWERX SOCIAL MEDIA LINKS

- [X/Twitter](#)
- [Facebook](#)
- [Instagram](#)
- [LinkedIn](#)
- [YouTube](#)