Basic Cyber Hygiene
FAR 52.204-21
The Proposed CMMC Level 1
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!
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/
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.
<table>
<thead>
<tr>
<th>AC</th>
<th>AT</th>
<th>AU</th>
<th>CM</th>
<th>IA</th>
<th>IR</th>
<th>MT</th>
<th>MP</th>
<th>PS</th>
<th>PE</th>
<th>RA</th>
<th>CA</th>
<th>SC</th>
<th>SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>3.2.1</td>
<td>3.3.1</td>
<td>3.4.1</td>
<td>3.5.1</td>
<td>3.6.1</td>
<td>3.7.1</td>
<td>3.8.1</td>
<td>3.9.1</td>
<td>3.10.1</td>
<td>3.11.1</td>
<td>3.12.1</td>
<td>3.13.1</td>
<td>3.14.1</td>
</tr>
<tr>
<td>3.1.2</td>
<td>3.2.2</td>
<td>3.3.2</td>
<td>3.4.2</td>
<td>3.5.2</td>
<td>3.6.2</td>
<td>3.7.2</td>
<td>3.8.2</td>
<td>3.9.2</td>
<td>3.10.2</td>
<td>3.11.2</td>
<td>3.12.2</td>
<td>3.13.2</td>
<td>3.14.2</td>
</tr>
<tr>
<td>3.1.3</td>
<td>3.2.3</td>
<td>3.3.3</td>
<td>3.4.3</td>
<td>3.5.3</td>
<td>3.6.3</td>
<td>3.7.3</td>
<td>3.8.3</td>
<td>3.9.3</td>
<td>3.10.3</td>
<td>3.11.3</td>
<td>3.12.3</td>
<td>3.13.3</td>
<td>3.14.3</td>
</tr>
<tr>
<td>3.1.4</td>
<td>3.2.4</td>
<td>3.3.4</td>
<td>3.4.4</td>
<td>3.5.4</td>
<td>3.6.4</td>
<td>3.7.4</td>
<td>3.8.4</td>
<td>3.9.4</td>
<td>3.10.4</td>
<td>3.11.4</td>
<td>3.12.4</td>
<td>3.13.4</td>
<td>3.14.4</td>
</tr>
<tr>
<td>3.1.5</td>
<td>3.2.5</td>
<td>3.3.5</td>
<td>3.4.5</td>
<td>3.5.5</td>
<td>3.6.5</td>
<td>3.7.5</td>
<td>3.8.5</td>
<td>3.9.5</td>
<td>3.10.5</td>
<td>3.11.5</td>
<td>3.12.5</td>
<td>3.13.5</td>
<td>3.14.5</td>
</tr>
<tr>
<td>3.1.6</td>
<td>3.2.6</td>
<td>3.3.6</td>
<td>3.4.6</td>
<td>3.5.6</td>
<td>3.6.6</td>
<td>3.7.6</td>
<td>3.8.6</td>
<td>3.9.6</td>
<td>3.10.6</td>
<td>3.11.6</td>
<td>3.12.6</td>
<td>3.13.6</td>
<td>3.14.6</td>
</tr>
<tr>
<td>3.1.7</td>
<td>3.2.7</td>
<td>3.3.7</td>
<td>3.4.7</td>
<td>3.5.7</td>
<td>3.6.7</td>
<td>3.7.7</td>
<td>3.8.7</td>
<td>3.9.7</td>
<td>3.10.7</td>
<td>3.11.7</td>
<td>3.12.7</td>
<td>3.13.7</td>
<td>3.14.7</td>
</tr>
<tr>
<td>3.1.8</td>
<td>3.2.8</td>
<td>3.3.8</td>
<td>3.4.8</td>
<td>3.5.8</td>
<td>3.6.8</td>
<td>3.7.8</td>
<td>3.8.8</td>
<td>3.9.8</td>
<td>3.10.8</td>
<td>3.11.8</td>
<td>3.12.8</td>
<td>3.13.8</td>
<td>3.14.8</td>
</tr>
<tr>
<td>3.1.9</td>
<td>3.2.9</td>
<td>3.3.9</td>
<td>3.4.9</td>
<td>3.5.9</td>
<td>3.6.9</td>
<td>3.7.9</td>
<td>3.8.9</td>
<td>3.9.9</td>
<td>3.10.9</td>
<td>3.11.9</td>
<td>3.12.9</td>
<td>3.13.9</td>
<td>3.14.9</td>
</tr>
<tr>
<td>3.1.10</td>
<td>3.2.10</td>
<td>3.3.10</td>
<td>3.4.10</td>
<td>3.5.10</td>
<td>3.6.10</td>
<td>3.7.10</td>
<td>3.8.10</td>
<td>3.9.10</td>
<td>3.10.10</td>
<td>3.11.10</td>
<td>3.12.10</td>
<td>3.13.10</td>
<td>3.14.10</td>
</tr>
<tr>
<td>3.1.11</td>
<td>3.2.11</td>
<td>3.3.11</td>
<td>3.4.11</td>
<td>3.5.11</td>
<td>3.6.11</td>
<td>3.7.11</td>
<td>3.8.11</td>
<td>3.9.11</td>
<td>3.10.11</td>
<td>3.11.11</td>
<td>3.12.11</td>
<td>3.13.11</td>
<td>3.14.11</td>
</tr>
<tr>
<td>3.1.15</td>
<td>3.2.15</td>
<td>3.3.15</td>
<td>3.4.15</td>
<td>3.5.15</td>
<td>3.6.15</td>
<td>3.7.15</td>
<td>3.8.15</td>
<td>3.9.15</td>
<td>3.10.15</td>
<td>3.11.15</td>
<td>3.12.15</td>
<td>3.13.15</td>
<td>3.14.15</td>
</tr>
<tr>
<td>3.1.16</td>
<td>3.2.16</td>
<td>3.3.16</td>
<td>3.4.16</td>
<td>3.5.16</td>
<td>3.6.16</td>
<td>3.7.16</td>
<td>3.8.16</td>
<td>3.9.16</td>
<td>3.10.16</td>
<td>3.11.16</td>
<td>3.12.16</td>
<td>3.13.16</td>
<td>3.14.16</td>
</tr>
</tbody>
</table>

- **AC**: Administrative Control
- **AT**: Administrative Technique
- **AU**: Administrative Procedure
- **CM**: Configuration Management
- **IA**: Information Assurance
- **IR**: Identity and Access Management
- **MT**: Mobile Device Management
- **MP**: Multi-Factor Authentication
- **PS**: Physical Security
- **PE**: Perimeter Security
- **RA**: Remote Access
- **CA**: Cloud Access
- **SC**: Supply Chain Management
- **SI**: Supply Chain Security

Legend:
- Orange: Administrative (e.g., policies, standards & procedures)
- Light Blue: Technical Configurations (e.g., security settings)
- Green: Software Solution
- Yellow: Assigned Tasks To Cybersecurity Personnel
- Blue: Assigned Tasks To IT Personnel
- Dark Blue: Assigned Tasks To Application/Asset/Process Owner
- Red: Configuration or Software Solution
- Gray: Configuration or Software or Hardware Solution

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.

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.
Check out this video on the Blue Cyber webpage.
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
Priority

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

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

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

* One solution, could be others.
<table>
<thead>
<tr>
<th>FAR 21 Requirement</th>
<th>NIST SP 800-171 Equivalent Requirement</th>
<th>NIST SP 800-171 Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>(b)(1)(ix)</td>
<td>3.10.5 Administrative Control</td>
<td>Control and manage physical access devices.</td>
</tr>
<tr>
<td></td>
<td>Physical Control</td>
<td></td>
</tr>
<tr>
<td>(b)(1)(x)</td>
<td>3.13.1 Hardware Solution*</td>
<td>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.</td>
</tr>
<tr>
<td>(b)(1)(xi)</td>
<td>3.13.5 Technical Control</td>
<td>Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</td>
</tr>
<tr>
<td>(b)(1)(xii)</td>
<td>3.14.1 Administrative Control</td>
<td>Identify, report and correct information and information system flaws in a timely manner.</td>
</tr>
<tr>
<td>(b)(1)(xiii)</td>
<td>3.14.2 Software Solution*</td>
<td>Provide protection from malicious code at appropriate locations within organizational information systems.</td>
</tr>
<tr>
<td>(b)(1)(xiv)</td>
<td>3.14.4 Technical Control</td>
<td>Update malicious code protection mechanisms when new releases are available.</td>
</tr>
<tr>
<td>(b)(1)(xv)</td>
<td>3.14.5 Software Solution*</td>
<td>Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.</td>
</tr>
</tbody>
</table>

* 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

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]?²⁵
- 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]?²⁶
Now Repeat, for each of the 17 Security Requirements

- Document your results
- Document your Artifacts
- Set a schedule to update
- Ask your questions
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](#)
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 OFFICE HOURS

• Register here: www.safcn.af.mil/CISO/small-business-cybersecurity-information/

• Nearly-daily opportunity to ask questions and get answers in-person.

• More information at https://www.safcn.af.mil/Contact-Us/
Every-Tuesday, Small Business Cybersecurity Ask-Me-Anything

WEEKLY – Every Tuesday 1pm Eastern

• Register here: www.sbir.gov/events

• A guest speaker will cover an ultra-relevant small business cybersecurity topic and get your cybersecurity/information protection questions answered.

• More information at https://www.safcn.af.mil/Contact-Us/
DAF CISO’s Deep Blue Cyber Line-Up

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!
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

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 – 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/
I have professional cybersecurity help for my small business.
**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 consult 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

---

**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