

AN OFFERING IN THE BLUE CYBER SERIES

Following the DFARS in your Small Business Contract



AFWERX

VERSION: March 2024

#9 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 CISO'S Blue Cyber

The DAF CISO's Blue Cyber Education Series for Small Businesses and Academic/Research Institutions is in its third year and has made over 20K outreach contacts in the U.S. Small Business ecosystem since April 2021.

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

CLICK BELOW FOR
VIDEOS

CLICK BELOW FOR
PRESENTATIONS

SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS

FOLLOWING THE CYBERSECURITY DFARS IN YOUR SMALL
BUSINESS CONTRACT

DOO CYBERSECURITY INCIDENT REPORTING

GET YOUR SPRS ONI 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 DOO CONTROLLED
UNCLASSIFIED INFORMATION (CUI)

DOO CLOUD COMPUTING

JAN 2024 DAF CISO'S SMALL BUSINESS
RESOURCES LOLLAPALOOZA +

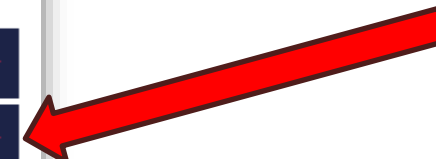
SMALL BUSINESS BLUE CYBER
EDUCATION SERIES PRESENTATIONS +

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 +



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 cybersecurity requirement which must be in place when you sign your contract.



Federal Acquisition Regulation (FAR) and DFARS

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

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

DFARS Clause
252.239-7010
Cloud Computing
Services

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

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

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

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

DFARS Clause
252.204-7021
Cybersecurity
Maturity Model
Certification
Requirement

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

DFARS Clause 252.239-7010 — 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.



So, when you sign your contract –
you are saying this is all complete.

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/portal/intranet/>



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/portal/intranet/>



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



Defense Industrial Base (DIB) Cybersecurity Portal

[Report a Cyber Incident](#)[DIB CS Member Login](#)[Cyber Incident Reporting](#)[FAQ](#)[Policy and Resources](#)[DC3](#)[DIB CS Program](#)[Weekly Cyber Threat Roundup](#)[Contact Us](#)

DIB CS Program Fact Sheet

[PDF Download](#)

DC3 Weekly Cyber Threat Roundup

[PDF Download](#)

DoD DIB Cybersecurity-as-a- Service (CSaaS) Services and Support

[PDF Download](#)

Obtain a Medium
Assurance Certificate

[More Info](#)

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

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

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 its interim plan to provide alternative, but equally effective, security measure is recorded in a Plan of Action with Milestones, called a POAM (NIST SP 800-171 security requirement 3.13.2)

NIST SP 800-171 System Security Plan (SSP)

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

1. SYSTEM IDENTIFICATION

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

1.1.1. System Categorization: Moderate Impact for Confidentiality

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

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

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

Name:	
Title:	
Office Address:	

Optional Template
available on NIST.Gov

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

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

Safeguard Covered Defense Information (CDI)



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

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

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

So, when you sign your contract –
you are saying this is all complete.

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

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

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

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

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

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

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

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

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

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

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

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

NIST SP 800-171 DoD Assessment Scoring Template

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

12

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



Self-Assessment



Submit information at <https://www.sprs.csd.disa.mil>



Flow the Requirement Down



Update your Self-Assessment

How to Enter a Basic Assessment Data into SPRS

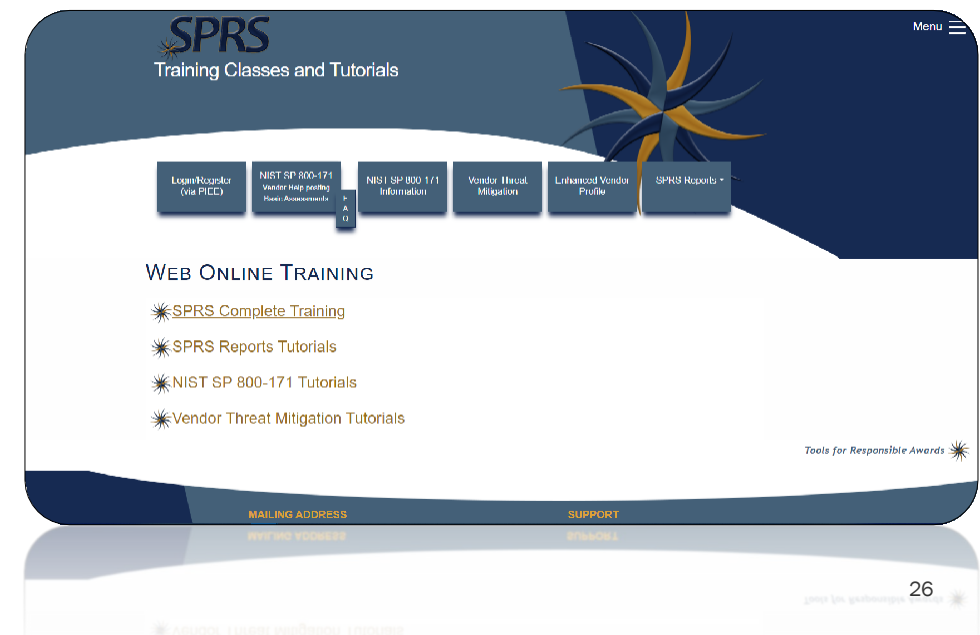
Post or email your business' summary level scores of a current NIST SP 800-171 DoD Assessment to SPRS for all covered contractor information systems relevant to the contract.

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

<https://www.sprs.csd.disa.mil/>



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... Date
04/06/2019	109	BASIC	NIST SP 800-171		ENTERPRISE	ELECTRONICS, INC. USA	07/30/2021	Network Security Plan	03/01/2019

1

Example output
of SPRS Basic Assessment

You Have Help with the new DOD CIO documents

Access Control (AC)

Level 1 AC Practices

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

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

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

Examine

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

Interview

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

DISCUSSION [NIST SP 800-171 R2]

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

FURTHER DISCUSSION

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

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

Example 1

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

Example 2

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

Potential Assessment Considerations

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

KEY REFERENCES



**UPDATES TO THE CMMC WEBSITE WILL BE
LIMITED DURING THE CMMC 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

CMMC Artifact Hashing Tool User Guide

- Under Development

New Documentation Guides

<https://dodcio.defense.gov/CM/CMC/Documentation/>

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

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

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



Can I Give My Contractor CUI?

DFARS 7012 “Adequate Security” Quote

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

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

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

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

So, when you sign your contract –
you are saying this is all complete.

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 2024 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.

Stay up-to-date at <https://dodcio.defense.gov/CMMC/>



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



CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE

Search Chief Information

HOME ABOUT DOD CIO IN THE NEWS LIBRARY CMMC CONTACT US


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

CYBERSECURITY MATURITY MODEL CERTIFICATION


CMMC 2.0

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

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




**CMMC 2.0
LAUNCHED**




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

LEARN MORE




**CMMC 2.0
PROGRAM**




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

LEARN MORE



**5 STEPS TO
CYBERSECURITY**



Actions your company can take today to protect against cyber threats

LEARN MORE

DFARS 252.204-7024

Use of Supplier Performance Risk System (SPRS) Assessments



Item Risk



Price Risk



Supplier Risk



Overall Risk

Prohibition on Contracting for some items

SBIR/STTR contract contains many requirements. Many talk to not contracting with certain entities for certain items.

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

Flows down to
Subcontractors

52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other

Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

- (1) Providing
- (2) Using

You must report exceptions

In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at <https://dibnet.dod.mil/portal/intranet/>

You must Flow the requirement down to subcontractors

All of these DFARS have many facets; this briefing is a high-level look

Covered article means any hardware, software, or service that—

- (1) Is developed or provided by a covered entity;
- (2) Includes any hardware, software, or service developed or provided In whole or in part by a covered entity; or
- (3) Contains components using any hardware or software developed I in whole or in part by a covered entity.

Covered entity means—

- (1) Kaspersky Lab;
- (2) Any successor entity to Kaspersky Lab;
- (3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
- (4) Any entity of which Kaspersky Lab has a majority ownership.

Flows down to
Subcontractors

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Prohibition

Prohibits the head of an executive agency, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception has been granted

- Nor may you enter into a contract, or extend or renew a contract, with a *Covered foreign country, which* means The People's Republic of China

Reporting requirement

In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information to the Contracting Officer, in the case of the Department of Defense, the Contractor shall report to the website

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

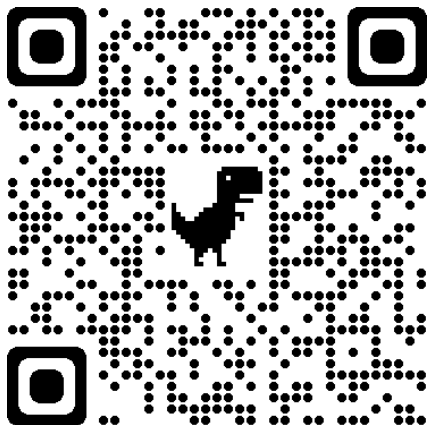
Website

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 CISO'S Blue Cyber

The DAF CISO's Blue Cyber Education Series for Small Businesses and Academic/Research Institutions is in its third year and has made over 20K outreach contacts in the U.S. Small Business ecosystem since April 2021.

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

- **REPORTING CONTRACTOR CYBER INCIDENTS**
- Modules on cybersecurity and information protection with links to all the Blue Cyber events are provided in the sections below
- Quick reference sheet of **Cybersecurity Resources**

If you have any questions please **contact us** and select "Small Business Cybersecurity."

