




Southwest Regional CIC
CMMC Implementation Conference

Presented by  **FutureFeed**

A background image showing several people sitting at a long wooden table in a workshop or office setting, working on laptops. The image is slightly blurred to emphasize the text overlay.

The CMMC EVERYTHING I Need to Know to Get Started GUIDE

Tools, Tips, and Tricks for Building a
Successful CMMC Program



Introduction

The FutureFeed platform was created to enhance our national security by enabling those in and beyond the defense supply chain to create fully managed information security programs compliant with not only legal and regulatory requirements, but also industry best practices. We are constantly enhancing FutureFeed with new capabilities which advance this mission.

At the same time, we know that even the best tools can only do a portion of the work. That is why we have a robust set of training built into the platform, and why we are proud to offer online and in-person educational options, including the **CMMC Implementation Conference (“CIC”)** series of conferences and this booklet. We hope this booklet answers many of your CUI and CMMC-related questions, and helps you identify additional resources that can aid you on your CMMC compliance journey. You can always E-mail questions to us at: Sales@FutureFeed.co

You can also join our weekly 15 Minutes with FutureFeed sessions, where we answer questions about CUI, CMMC, NIST SP 800-171, cybersecurity, compliance, the FutureFeed platform, and much more. To register, visit: <https://FutureFeed.co/15>

Good luck on your CMMC compliance journey! We hope you will let us help take some of the stress out of that journey.

Sincerely,
The FutureFeed Team

CMMC Ecosystem Overview

From start to finish, CMMC Level 2 journey takes 12-18+ months. The ecosystem is ready to accelerate your CMMC journey.

CMMC Ecosystem by the Numbers

Ecosystem Role	Organizations and People	Nov. 2023
Help You Prepare	Registered Provider Organizations	310
	Registered Practitioners	1359
	Registered Practitioners (Advanced)	105
Assess and Certify	Authorized C3PAOs	48
	Certified CMMC Professionals (CCPs)	592
	Certified CMMC Assessors (CCAs)	166

Getting a Head Start

Joint Surveillance Voluntary Assessment participants should receive CMMC certifications once the process begins.

Outpacing Their Competition	Joint Surveillance Voluntary Assessments Conducted	~40
	Joint Surveillance Voluntary Assessments Pending	125+

Contents

Introduction.....	i
CMMC Overview	ii
CMMC Ecosystem by the Numbers	ii
Getting a Head Start	ii
Southwest Regional CIC Agenda.....	1
Speakers and Contact Information	2
Supply Chain Management Concerns in Government Contracts .	7
What are the Typical Government Requirements?	8
Can Agencies Create their own Requirements?	8
What are Mandatory Contract Clauses?	9
What are Mandatory Flow Down Clauses?	9
What Impact can Noncompliance Have?.....	9
What is DoD Doing to Encourage/Require Compliance?	10
How Much Trouble can a Contractor Face if they have not Implemented the Security Requirements?	11
How can DoD or DoJ Catch Noncompliant Contractors?	12
What are Whistleblowers?	12
We Don't Handle CUI; Why is Our Prime Asking us to Submit a Score to SPRS?.....	13
What Information is Collected in SPRS?	13
What Information can Prime Contractors ask for?	13
Must I give a Prime Contractor Everything they ask for?	14
Why are Prime Contractors Pushing their Subcontractors to Earn Higher Scores for SPRS?	14
FCI Federal Contract Information.....	15

What is Federal Contract Information (FCI)?..... 16

What are Some Examples of FCI? 16

CUI Controlled Unclassified Information 17

What is Controlled Unclassified Information? 18

What are Some Examples of CUI? 18

CUI Basic and CUI Specified...What’s the Difference?..... 18

How do I know if Something is CUI? 19

How will I Know if Information I Create is CUI? 21

Is all Legacy Information (e.g., FOUO) Automatically CUI? 21

To Whom can CUI be Disseminated? 21

Where can I Learn More About CUI? 22

CMMC Cybersecurity Maturity Model Certification 23

What is CMMC? 24

Does CMMC Apply to all Government Information? 24

Is all Unclassified, Non-Public Information Treated the Same Under CMMC? 24

How does CMMC Help Ensure the Safeguarding of FCI and CUI? 24

When is an Organization Subject to a Given CMMC Level? 25

Where can I Learn More about CMMC? 26

What is the relationship between FCI, CUI, CMMC, and NIST SP 800-171 and NIST SP 800-171A?..... 26

When will CMMC Certifications be Required? 27

Should I wait for the CMMC rules to be published before I begin reviewing and enhancing my information security program? . 28

Should I wait for NIST SP 800-171r3 to be finalized before I begin reviewing and enhancing my information security program? 29

Are There any Non-Government Resources that can Help us Create a CMMC Compliance Program?	29
Can any Third Parties Provide Complete (i.e. 100%) CMMC Services?	29
CMMC Assessment FAQs	31
Building Your CMMC Compliance Program.....	33
How do I Create a CMMC Compliance Program?	34
Decide: DIY or Get Help.....	34
Choose Your Tool	36
Find the FCI and CUI	37
Determine: CMMC Level 1, 2, or 3?	38
Establish a System Security Plan (“SSP”) Framework.....	39
Inventory Your Assets	39
Define Current and Desired Scope.....	40
Identify Gaps and Create POA&Ms.....	41
Close POA&Ms	44
Validate	47
Certify	47
Maintain	47
Why should I use a tool like FutureFeed as Part of My Compliance Program?	47
Official Federal Resources	49
Key CMMC	52
Tools and Resources	52
Acronyms	57

Copyright 2023 Continuous Compliance LLC dba FutureFeed, All Rights Reserved

First Edition

“FutureFeed” and the FutureFeed logo are trademarks of Continuous Compliance.

All writing, opinions, and purported statements of fact are solely from and due to the authors’ personal experience and research. Readers should not construe any statements contained herein to be from or endorsed/approved by any CIC sponsors or exhibitors. All writing and statements are the sole responsibility of the author.

Although the authors have made every effort to ensure that the information in this book was correct at press time, neither Continuous Compliance nor the authors assume, and all parties hereby disclaim, any and all liability to any party for any loss, damage, or disruption caused by any errors or omissions in this book, whether such errors or omissions result from negligence, accident, or any other cause.

Southwest Regional CIC

Agenda

8:00 AM	Check-in & Breakfast
8:30 AM	Welcome & Keynote
9:00 AM	State of the State: DCMA DFARS 7012/CUI Policy & Enforcement
10:00 AM	Break
10:10 AM	The Carrot and the Stick: Prime Contractor Supply Chain Strategy Panel
11:00 AM	Why are we Here? CUI
11:45 AM	Lunch Break/Networking
12:30 PM	What Does Success Look Like (and Mean in Dollars)? DIB Supply Chain Panel
2:00 PM	How Do I Start? Implementation Training & Education
2:45 PM	Um...I Need Help! Is Your Current Service Provider the Right Service Provider?
3:30 PM	Brand NEW World. New Expectations.
4:00 PM	Living in a Documented World: Culture Change to Make Compliant Cyber Work
4:45 PM	Your World Through the Assessor's Eyes: Assessment Preparation, External Service Providers Support to Assessments
5:30 PM	Resources and Wrap-up
5:45 PM	Happy Hour and Networking

Speakers and Contact Information



Tommy Baril

U.S. Government
Accountability Office

Defense Capabilities and
Management Team

BarilT@GAO.gov

Mark Berman

FutureFeed

MBerman@FutureFeed.co





Eric Crusius

Holland & Knight

Eric.Crusius@HKLaw.com

Regan Edens

DTC Global

ReganEdens@DTCGlobal.us



George Finney

Southern Methodist University

Andrew Gentin

U.S. Department of Justice

Andrew.Gentin@USDOJ.gov



Jim Goepel

FutureFeed

JGoepel@FutureFeed.co

Stuart Itkin

NeoSystems

Stuart.Itkin@NeoSystemsCorp.com





Jerry Leishman

CROWN Information Security

Jerry.Leishman@CROWNInfosec.com

Lincoln Neely

Beryllium Infosec

Lincoln@BerylliumInfosec.com



Mitch Niemela

Toolcraft Inc.

Mitch@TCPrecision.com



Robert Teague

Clearwater/Redspin

Robert.Teague@Redspin.com



Matt Travis

The Cyber Accreditation Body
(Cyber AB)

MTravis@CMMCAB.org



Fred Tschirgi

Summit 7

Fred.Tschirgi@Summit7.us

Supply Chain Management Concerns in Government Contracts



The United States Government purchases goods and services from a vast number of organizations around the world. These organizations form the government's "supply chain."

As we saw during the global pandemic, issues in the supply chain can create ripple effects across the entire nation. They can even place our national security at risk. The government addresses these risks by adding requirements to its commercial contracts.

When the United States Government purchases goods or services from those in its supply chain, it always does so with a single entity: the **"prime contractor."** Although the prime contractor may hire others to fulfill (i.e., "subcontract out") portions of the contract's requirements, the prime contractor remains directly liable for these subcontractors' actions.

As a result, many prime contractors are careful to ensure that their contracts with their subcontractors **"flow down"** (i.e., pass along or include) all of the requirements from the contract with the government. Prime contractors also look for ways to validate that the subcontractors are meeting those contractual requirements and hold the subcontractors accountable when they are not in compliance.

What are the Typical Government Requirements?

Writing contracts is tricky. To streamline that process and standardize the requirements across the millions of contracts that it enters into each year, the government created a set of pre-written contract clauses. These requirements can be found in the **Federal Acquisition Regulations ("FAR").**

Can Agencies Create their own Requirements?

Yes. While the FAR provides a high-level acquisition framework, many agencies need to tailor the requirements, or add other requirements, because of the agencies' unique attributes. For

the **United States Department of Defense (“DoD”)**, these requirements are published in the **Defense Federal Acquisition Regulations Supplement (“DFARS”)**.

What are Mandatory Contract Clauses?

As they write **Requests for Information (“RFIs”)**, **Requests for Proposals (“RFPs”)**, and the resulting contracts, Contracting Officers select the appropriate clauses from the FAR and DFARS based on the nature of the work being performed under the contract. In some cases, the government has identified the requirements in certain clauses to be so important that they must be incorporated into all contracts. These mandatory clauses address various factors, such as payment terms.

What are Mandatory Flow Down Clauses?

In some cases, contract requirements are so important to the government that they require prime contractors to always flow down the requirements to all subcontractors. In general, these clauses must be in every subcontract. These clauses include, for example, [FAR 52.204-21](#), which covers the basic safeguarding requirements for **Federal Contract Information (“FCI”)**.

In certain, limited cases, although the clauses are required, the government allows the prime contractor to not flow down the clause, but only if very specific conditions are met. For example [DFARS 252.204-7012](#) need not be included when the contract does not involve **Covered Defense Information (“CDI”)** or other **Controlled Unclassified Information (“CUI”)**.

What Impact can Noncompliance Have?

Failure to comply with contractual requirements, regardless of whether the noncompliance is by the prime contractor or a subcontractor, puts the prime contractor in breach of the contract with the government. This can result in significant consequences for the prime contractor, including fines and

penalties, termination of contracts, nonrenewal of existing contracts, and debarment.

What is DoD Doing to Encourage/Require Compliance?

DoD is pushing its supply chain to comply with all aspects of contracts, with particular attention to cybersecurity. One motivation for this is that DoD faces its own legal obligations associated with CUI. DoD needs to ensure that its contractors can properly protect CUI when it is created by the contractors or received from the government, otherwise the failure to properly protect the information can create legal issues for DoD.

Another motivation is to protect our warfighters. Many contractors are handling information that is valuable to our adversaries. When contractors do not protect CUI appropriately, our adversaries can steal the information. This allows them to more easily target our warfighters and compete with them on the battlefield, making conflicts last longer and more deadly.

Given these and other pressures, DoD introduced two major cybersecurity initiatives over the past few years. One of them is a short-term fix, and the other is a much larger program.

The short-term initiative is embodied in the clauses at [DFARS 252.204-7019](#) and [DFARS 252.204-7020](#). The [-7020](#) clause requires all contractors who handle CUI to self-assess their compliance with certain cybersecurity requirements and to report a resulting score to the [Supplier Performance Risk System](#) (“SPRS”). The score, which can range from -203 to 110, is calculated based on the requirements that have yet to be implemented. That is, you start with 110 points and lose 5, 3, or 1 point for each applicable requirement that is not fully met. DoD’s goal is for all contractors who handle CUI to achieve (honest) 110-point scores in SPRS.

As a mechanism for addressing the potential fraud that goes along with self-assessments and reporting, DoD also introduced the -7019 clause. The [-7019](#) clause allows DoD to audit any contractor, including subcontractors, to confirm that the contractor's stated score is accurate.

The longer-term initiative is the [Cybersecurity Maturity Model Certification](#) (“CMMC”) program. Under CMMC, all DoD contractors will be required to perform self-assessments of their cybersecurity program against other requirements. A member of the senior management team must then submit an annual attestation that the company complies with those requirements.

In addition, DoD will soon require all contractors who handle CUI, with limited exceptions, [to obtain a CMMC certification](#). The CMMC certification, which must be issued by an authorized third party, validates the contractor's compliance with appropriate cybersecurity requirements and that the contractor can properly safeguard the government's information. All required CMMC attestations and certifications must be in place before the contract is awarded.

How Much Trouble can a Contractor Face if they have not Implemented the Security Requirements?

Over the past four administrations, the United States Government has taken progressively stronger stances which evidence the important role information security and cybersecurity play in the country's national security. As part of that process, in October of 2021 the [United States Department of Justice](#) (“DOJ”) announced its “[Civil Cyber Fraud Initiative](#)” in which it began more aggressively identifying and pursuing contractors who are not meeting the cybersecurity and information security protection requirements defined in their government contracts.

Although the Civil Cyber Fraud Initiative is still in its infancy, it is already yielding results, including several [multi-million-dollar settlements](#).

Contractors should also be aware that, under the False Claims Act, the government can fine contractors up to 3x the value of the corresponding contract **PLUS** \$11,000+ per “claim” for misrepresenting the contractor’s compliance with material contractual provisions like the cybersecurity and information security clauses. Contractors can even face other actions, including being debarred (prohibited from participating on future contracts) and the termination of existing contracts.

How can DoD or DoJ Catch Noncompliant Contractors?

There are several ways, including when:

- the contractor is the victim of a cyber incident, and the perpetrators publish information about the contractor and their deficiencies online (e.g., after the contractor refuses to pay a ransom);
- the contractor is a victim of a cyber incident and reports the incident to DoD who, while performing an audit to determine the scope of any damage, identifies material deficiencies;
- the contractor’s own actions make it clear to DoD that certain requirements are not met (e.g., the contractor sends unencrypted/improperly encrypted CUI via E-mail to a DoD employee); or
- an employee of the contractor reports the contractor’s noncompliance to DoD (i.e., they are a “whistleblower”) or takes up the case on their own.

What are Whistleblowers?

In this context, whistleblowers are people with inside knowledge of a government contractor’s noncompliance. Whistleblowers must attempt to get the contractor to resolve the noncompliance first but, if that does not happen, the whistleblower can report the

noncompliance to the government. They can even bring a lawsuit on behalf of the government.

Whistleblowers can receive up to 25-33% of any financial settlement or court-awarded damages that arise from the reported case. These strong financial incentives, coupled with increasing awareness of compliance requirements, have resulted in a significant increase in the number of whistleblower cases.

We Don't Handle CUI; Why is Our Prime Asking us to Submit a Score to SPRS?

When a contract is awarded, the prime contractor attests to the fact that all contractors handling CUI on the contract have submitted scores to SPRS. Since there is a lot of confusion about what constitutes CUI, many prime contractors are simply assuming that all of their subcontractors will handle CUI. They are therefore requiring all subcontractors to perform self-assessments and record scores in SPRS.

What Information is Collected in SPRS?

When you submit your score to SPRS, the government only asks for some basic information, such as your company name, [Commercial and Government Entity](#) (“**CAGE**”) code, and score. The government does not want to be a repository for contractors’ [System Security Plans](#) (“**SSPs**”), [Plans of Action and Milestones](#) (“**POA&Ms**”), or other security-related information.

What Information can Prime Contractors ask for?

As commercial entities, the prime contractors can largely set whatever requirements they like for determining who should qualify as a subcontractor. They can, therefore, ask for a lot of information, including your current SPRS score, your SSP, and your POA&Ms.

Must I give a Prime Contractor Everything they ask for?

Not necessarily. As a practical matter, you can always push back and ask why they need the information, how it will be protected, etc. before you share it with them. However, the prime contractor can also choose not to do business with your company.

One way to help mitigate some of the risk is through a platform like [FutureFeed](#). You can give specific individuals in the prime contractor's company access to the information they need for a limited time, allowing them to gain their desired level of confidence while still allowing you to control your information.

Why are Prime Contractors Pushing their Subcontractors to Earn Higher Scores for SPRS?

Back in 2020, DoD knew that it needed to make some changes to the way it evaluates proposals. DoD recognized that its traditional "lowest cost, technically acceptable" acquisition approach, and even some versions of the "best value" approach, created an inequity.

Under these traditional acquisition approaches, contracts were typically awarded with lowest cost as a leading factor. However, contractors who did the right thing and implemented the required security faced higher operating costs. As a result, these same contractors were essentially penalized because they did the right thing. So, DoD created [DFARS 252.204-7024](#).

The -7024 clause allows Contracting Officers to take information in SPRS, as well as other supply chain security information, into account when making an award. This allows the Contracting Officer to award contracts to those contractors, and contractor teams, who are taking the right steps to protect CUI. This is true even when the price of their goods or services is (within reason) higher than their competitors. Prime Contractors want to know the score their subcontractors have recorded in SPRS so they can better assess their chances of successfully winning a proposal.

FCI

Federal Contract Information



What is Federal Contract Information (FCI)?

The **Federal Acquisition Regulations** (“**FAR**”) define **Federal Contract Information** (“**FCI**”) as “...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.” [[FAR 52.204-21\(a\)](#)]

Put more simply, FCI is any nonpublic information that a contractor creates for, or receives from, the government under a contract.

What are Some Examples of FCI?

Almost everything you create or receive under a government contract is FCI. This includes early drafts of deliverables and even E-mails with government employees.

CUI

Controlled Unclassified Information



What is Controlled Unclassified Information?

The CUI program defines CUI as “...information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see definition above) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.” [\[32 CFR 2002.04\(h\)\]](#)

Put more succinctly, CUI is unclassified information which a law, regulation, or government-wide policy (“**LRGWP**”) requires to be protected.

What are Some Examples of CUI?

Over 400 LRGWPs are formally authorized to serve as the basis for designating information as CUI. They cover a wide range of the government’s information, including:

- law enforcement investigations and court proceedings;
- personnel records, student records, and genetic information;
- naval nuclear propulsion information; and
- information about corporate mergers, net worth, and retirement accounts.

Even E-mails can rise to the level of CUI depending on their content.

CUI Basic and CUI Specified...What’s the Difference?

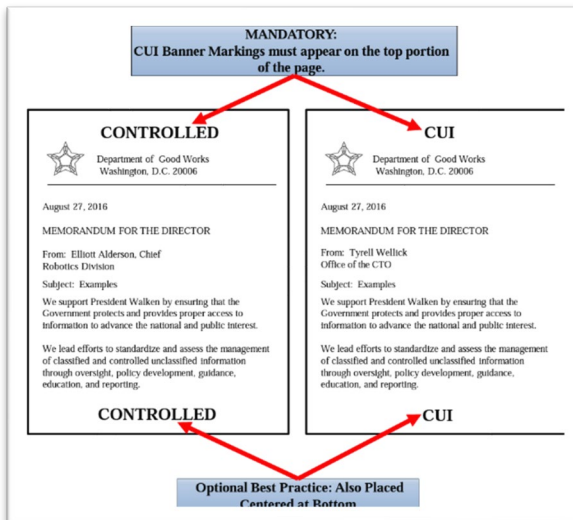
Information is “**CUI Specified**” if the applicable LRGWP says the information can or must be safeguarded in a particular way, or that the information is subject to limited dissemination controls.

For example, information that is subject to the [International Traffic in Arms Regulations](#) (“**ITAR**”) is CUI Specified because ITAR prohibits the dissemination of that information outside the United States, including to non-US persons, without a license.

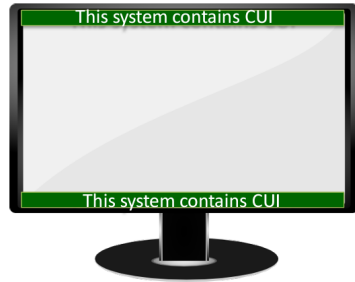
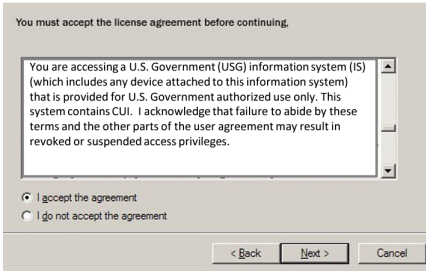
If the LRGWP does not specify safeguarding or limited dissemination controls, then the information is “**CUI Basic**”.

How do I know if Something is CUI?

In most cases, information will be conspicuously marked with either “CUI” or “Controlled” in the header of the document or on the media containing the information if the information is CUI.



In some cases, such as where it is not possible to directly mark the information, it may be indirectly “marked” as CUI via language in a contract, appendix, memorandum, separate agreement, or other document. In other cases, the container or room in which the information is stored may be marked, rather than the information itself.



The [National Archives and Records Administration](#) (“NARA”) has published a [CUI Marking Handbook](#) that contains useful information about how to properly mark CUI. You can find links to the CUI Marking Handbook and other resources at the end of this booklet.

As a [Department of Defense](#) (“DoD”) contractor, you should be on the lookout for information marked with [DoD Distribution Statements B-F](#). If you find any information with those markings, you should treat that information as CUI even if it is not marked with CUI markings. The fact that the information contains one of those Distribution Statements inherently makes it CUI.

Anatomy of a Distribution Statement



- | | |
|---|---|
| 1. Authorized Audience or Who Can Access | 3. Date of Determination |
| 2. Reason for Control or Why/Reason | 4. Controlling Office or Releasing Authority |

How will I Know if Information I Create is CUI?

Your contract with the government will tell you. In fact, it should not only tell you specifically which information you create is CUI, but it should also tell you how to mark the information, including an appropriate “designation indicator,” and the corresponding LRGWP(s) that are the basis for designating the information CUI.

DoD contractors should note that, as discussed above, if their contract requires them to create information and mark that information with one or more of DoD’s Distribution Statements B-F, that information has been designated as CUI and should be handled as such. You should ask your Contracting Officer for appropriate CUI markings if they have not been provided.

Is all Legacy Information (e.g., FOUO) Automatically CUI?

No. Under the CUI program, the agency which created or owns the information must determine whether any information that contains legacy markings, such as **Sensitive but Unclassified (“SBU”)**, **For Official Use Only (“FOUO”)**, **Law Enforcement Sensitive (“LES”)**, etc., is CUI.

If an agency determines that legacy information is CUI, the agency must mark it appropriately before disseminating the information outside the agency. If the legacy information is in a contractor’s possession, the agency must tell the contractor how to properly mark the information, and the contractor should ask the agency for the LRGWP that is the basis for the CUI designation. If the information is CUI Specified, then the anyone handling it has additional safeguarding obligations. The only way for a contractor to be certain they are meeting those extra obligations is by knowing exactly which LRGWP applies.

To Whom can CUI be Disseminated?

Only those with a Lawful Government Purpose are authorized to access (including receive) CUI. **Lawful Government Purpose** is

defined as “any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).” [\[32 CFR 2002.04\(bb\)\]](#)

Although Lawful Government Purpose is a much broader standard than the “need-to-know” standard used for classified information, it is critical that contractors ensure that they only disseminate CUI to (and allow CUI to be accessed by) appropriate persons whose access will further the purpose of the corresponding contract. For example, the cleaning crew in an office most likely does not have a Lawful Government Purpose to access most CUI, and therefore steps should be taken to keep the cleaners from accessing CUI in the contractor’s environment.

Where can I Learn More About CUI?

NARA oversees the CUI program and maintains the authoritative list of all of the LRGWPs that can be the basis for a CUI designation. This list is referred to as the “[CUI Registry](#),” and is a useful resource for contractors to better understand the different categories of information that an agency can designate as CUI.

In addition, [NARA](#) and [DoD](#) both offer free online CUI training. This training covers how to mark information as CUI once an agency has designated the information as CUI. DoD’s training is mandatory for any contractor who handles CUI. Be sure you take the test and keep a copy of the certificate (assuming you pass) at the end. Links to the DoD and NARA CUI training can be found at the end of this booklet.

For more details on CUI and the CUI program, the books [CUI Fundamentals](#) and [CUI Informed](#) by James Goepel (available from your favorite bookseller or <https://CUIinformed.com>) cover the CUI program in more detail than we can in this booklet.

CMMC

Cybersecurity Maturity Model Certification



What is CMMC?

The CMMC program is DoD's approach to ensuring that the federal government's non-public, unclassified information is properly protected when that information is given to, or created by, government contractors.

Does CMMC Apply to all Government Information?

Technically, no. CMMC does not apply to information which the government makes publicly available, nor does it apply to classified information. As a practical matter, however, CMMC will apply to most of the information DoD contractors create or receive under a contract with DoD.

Is all Unclassified, Non-Public Information Treated the Same Under CMMC?

No. Contractors must protect all non-public, unclassified information (i.e., FCI) using the 15 basic safeguarding requirements defined in [FAR 52.204-21](#). [CMMC Level 1](#) is focused on ensuring contractors properly safeguard FCI.

CUI carries with it additional safeguarding requirements mandated by the CUI program. [CMMC Levels 2 and 3](#) help DoD ensure that DoD only entrusts CUI to contractors who can and will properly safeguard that information.

How does CMMC Help Ensure the Safeguarding of FCI and CUI?

Under the CMMC program, DoD contractors are required to review their information security programs against certain requirements to ensure that the programs meet (i.e., comply with) those requirements. Contractors are required to submit self-attestations of continued compliance with the requirements on an annual basis.

In addition, most contractors storing, processing, or transmitting CUI will be required to have an authorized [CMMC 3rd Party Assessment Organization](#) (“C3PAO”) conduct an assessment of the contractor’s information security program and certify that the program meets the published requirements. These certifications are valid for three years.

CMMC Model 2.0		
	Model	Assessment
LEVEL 3	110+ requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171	Triennial third-party assessment & annual affirmation; Triennial self-assessment & annual affirmation for select programs
LEVEL 1	15 requirements	Annual self-assessment & annual affirmation

When is an Organization Subject to a Given CMMC Level?

CMMC is comprised of three levels. Level 1 applies to all DoD contractors. All contractors are required to implement the fifteen (15) information security requirements defined in [FAR 52.204-21](#). All contractors must submit a self-attestation to DoD confirming that they have properly and completely implemented the requirements. DoD estimates that approximately 220,000 companies will need to comply with CMMC Level 1 requirements.

Level 2 applies to all government contractors who handle CUI. These contractors, with limited exceptions, are required to obtain third-party certifications of their compliance with the requirements in [NIST SP 800-171](#) before the contractors can be

awarded, or participate in, a contract. DoD estimates that approximately 80,000 companies will need to comply with the CMMC Level 2 requirements.

Level 3 applies to government contractors who handle some of the most sensitive CUI. In addition to obtaining a CMMC Level 2 certification from a C3PAO, these contractors must also undergo an audit by DoD's [Defense Industrial Base Cybersecurity Assessment Center](#) (“**DIBCAC**”) team to validate that the contractor has implemented select requirements from [NIST SP 800-172](#). DoD estimates that approximately 300 companies will need to comply with the Level 3 requirements.

Where can I Learn More about CMMC?

The CMMC regulations can be found in the [Code of Federal Regulations](#) (“**CFR**”). They are often referenced by the name of the CFR volume in which they appear, such as the FAR or DFARS. The most up to date, official versions of the CMMC requirements documents (e.g., the CMMC Assessment and Scoping Guides) can be found on the [DoD CIO](#) website.

The website of the [Cyber AB](#), the DoD-authorized organization which is responsible for managing the CMMC ecosystem, has useful information about CMMC and the various [entities and individual certifications](#) that exist in the ecosystem.

The book “[CMMC Simplified](#)” by Fernando Machado offers a high-level overview of the CMMC program and is a great resource for those new to CMMC.

What is the relationship between FCI, CUI, CMMC, and NIST SP 800-171 and NIST SP 800-171A?

The CMMC program was created to ensure CUI and FCI are properly protected by government contractors. [FAR 52.204-21](#) establishes the fifteen basic requirements that all contractors who handle FCI (which is essentially all contractors) must meet.

The CUI program establishes the requirements in [NIST SP 800-171](#) as the minimum protections that must be in place to protect CUI in contractor information systems. It also establishes [NIST SP 800-171A](#) as the assessment guide for determining whether the requirements in [NIST SP 800-171](#) have been met.

When a CMMC assessment team reviews your information security program, they will be validating not only that your program meets the requirements defined in [NIST SP 800-171](#), but also that you have done so by satisfying the “assessment objectives” associated with each requirement in [NIST SP 800-171A](#).

When will CMMC Certifications be Required?

The answer to this question is subject to change. DoD recently completed the government’s internal regulatory review process to update the CMMC program. However, as of the publication of this booklet, the resulting regulation is not publicly available. When that is made public, we expect DoD to announce additional timing and implementation details.

Since CMMC’s inception in 2019, DoD has been warning contractors that CMMC will appear in all contracts [starting in FY2025](#). DoD would therefore be justified in keeping that 2025 implementation deadline in place for all contracts.

However, there are a few legal and practical issues that will likely prevent CMMC from appearing in every contract starting in FY2025. Instead, when it goes into effect, DoD will likely begin implementing CMMC as part of a phased roll-out over 3-5 years. At most, CMMC requirements will likely only appear in a limited number of contracts in FY2024. We will likely see a steady, and perhaps even exponential, increase in the number of contracts with CMMC requirements over the subsequent 3-5 years, with CMMC embedded in every contract somewhere between FY2028 and FY2030.

Should I wait for the CMMC rules to be published before I begin reviewing and enhancing my information security program?

No. And for several reasons.

As discussed above, Contracting Officers are already able to award contracts based on your current score in SPRS. You can increase the odds of a successful award by ensuring that your proposal teammates and you all have (legitimate) high scores in SPRS.

In addition, when DoD Contracting Officers create a **Request for Proposals** (“RFP”) or **Request for Information** (“RFI”), they include not only a description of work to be performed or the goods to be purchased, but also a set of contract “clauses” which are pulled from the FAR and/or the DFARS. Regardless of whether these clauses are written out in full (i.e., expressly incorporated) or simply referenced in the contract (i.e., incorporated by reference), they become part of the contract with the government, and the contractor is obligated to meet those requirements.

The clause at [FAR 52.204-21](#) is a required clause, meaning it must be incorporated into every government contract. This clause defines a basic set of information security protections that all contractors are expected to have in place. [FAR 52.204-21](#) has been in effect since June 16, 2016.

In addition, the clause at [DFARS 252.204-7012](#) requires that contractors who handle CUI implement [NIST SP 800-171](#). This requirement has been in effect since 2017.

If you are a DoD contractor with an active contract, you likely have been contractually attesting to meeting these requirements. This carries with it significant risk if you are found to be noncompliant. Therefore, it is essential that you begin your compliance journey ASAP.



Should I wait for NIST SP 800-171r3 to be finalized before I begin reviewing and enhancing my information security program?

No. Although NIST expects to publish the final versions of [NIST SP 800-171r3](#) and [NIST SP 800-171Ar3](#) in Q1 2024, it will likely take some time (at least another 6-9 months) before DoD will require contractors to meet the requirements in [NIST SP 800-171r3](#). In the meantime, as discussed above, contractors are already expected to comply with the requirements in [FAR 52.204-21](#) and [NIST SP 800-171r2](#). Waiting only increases the likelihood that the government will catch the contractor with a program that does not meet the requirements.

Are There any Non-Government Resources that can Help us Create a CMMC Compliance Program?

Yes. There are nonprofit organizations, like the [CMMC Information Institute](#), which publish low and no cost tools and resources for contractors. There are also organizations like [Parabilis](#) which can help contractors secure funding needed to improve their information security programs. In addition, there are many cloud-based service providers who offer tools and services which can significantly accelerate the CMMC compliance process. There are also many consultants and managed IT and security service providers who can help you understand and meet the requirements that you cannot, or are not willing to, outsource to a cloud provider.

Can any Third Parties Provide Complete (i.e. 100%) CMMC Services?

No, and you should be very wary of any organization that claims that it can. There are, inherently, certain requirements that only your organization can meet. For example, one objective in [NIST SP 800-171A](#) is the identification of all authorized users for systems that handle CUI. A third party can help you add and

remove accounts from those systems, but the third party does not know whether a particular account belongs to someone who is authorized to access CUI. Only your organization can make that determination.

CMMC Assessment FAQs



How Invasive is a CMMC Assessment?

Many people seem to think that CMMC assessors will run rampant through their offices, rummaging through filing cabinets and IT systems on the hunt for mishandled CUI. That simply is not the case.

A CMMC assessment is not overly invasive. The assessment team will need to speak with your people and, in many cases, tour your facilities. However, if your compliance program is well-structured and properly documented, the “live” portion of the assessment (part of which may be conducted via video conference) will likely be completed in a week or less.

What Should I Expect During a CMMC Assessment?

The process begins with the contractor interviewing one or more C3PAOs. The goal of the interview is to find someone who is familiar with the overall structure of the contractor’s business. For example, if the contractor is a manufacturing business, the contractor might want to select a C3PAO who is familiar with CNC and other equipment and the issues involved with maintaining such equipment.

Once a C3PAO is selected, the contractor will give the C3PAO access to, or copies of, the contractor’s SSP and related documents. The Lead Assessor will review those documents to ensure that there is adequate and sufficient evidence to proceed with the assessment.

The next step is for the assessment team to review the documentation in detail, requesting additional information if necessary. Interviews and testing are then conducted.

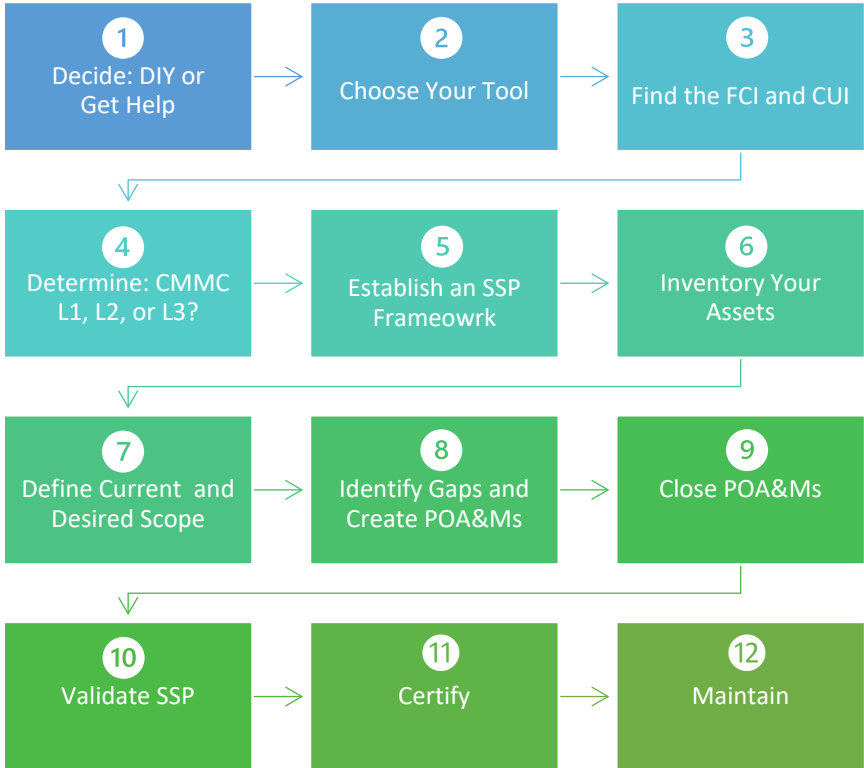
The Assessment Team will provide the contractor with status updates at the end of each day during the “live” portion of the assessment. The contractor may have the opportunity to correct minor deficiencies during the assessment.

Building Your CMMC Compliance Program



How do I Create a CMMC Compliance Program?

The process for creating a CMMC Compliance program is straightforward, and is defined by twelve basic steps:



Let's walk through some of the basics from each step.

1
Decide: DIY or
Get Help

Decide: DIY or Get Help

The first step in this process is to decide whether you are going to try to do this alone or if you are going to bring in outside help.

As discussed above, there are certain requirements that simply cannot be outsourced. However, there are many highly qualified persons who are ready to help guide you through the things that

you need to do and will take the burden of doing the other things for you.

If you are somewhat technically proficient, the CMMC Information Institute has [published a list of requirements](#) that can reasonably be implemented by a small or medium-sized business, and those which should likely be outsourced to more qualified persons. If you decide to do everything yourself, we encourage you to attend a Cyber AB [Certified CMMC Professional](#) (“CCP”) course taught through a Cyber AB [Licensed Training Provider](#) (“LTP”) to gain a better understanding of the CMMC program and CMMC assessment expectations. SMU is an official LTP and offers the [CCP](#) and [CCA](#) programs.

If you decide to outsource, you have a few different options, and you can choose one or more of them. For example, there are a cadre of highly-knowledgeable consultants who can assist you with building a CMMC program. There are also organizations which are increasingly specializing in providing managed IT and/or security services for those in the critical infrastructure space, including government contractors. These Mission Critical Service Providers often have at least one CCP or [Certified CMMC Assessor](#) (“CCA”) on staff, even if those organizations do not conduct formal CMMC assessments.

In addition to managed services, you may also want to consider cloud-based services. There are a variety of services available, some of which are targeted toward those with specific needs (e.g., secure E-mail and/or file sharing) while others are more general. Typically, the more targeted offerings are less expensive.

When selecting a cloud-based service, it is important to note that, if that cloud service will be handling CUI, it must be FedRAMP authorized at the moderate impact level or have equivalent security. The [Federal Risk and Authorization Management Program](#) (“FedRAMP”) is the government’s

program for validating that cloud services can properly protect the government's information.

The [FedRAMP Marketplace](#) lists those services which have received an [Authorization to Operate](#) (“ATO”), meaning that they are cleared for use by at least one agency. The [FedRAMP Marketplace](#) listing also includes the impact level at which the offering can operate. If you use the [FedRAMP Marketplace](#) to select a cloud service, be sure to look for the Moderate (or High) impact level if that service will handle CUI.

Although the number of FedRAMP-authorized cloud services is steadily increasing, it is still very small compared to the universe of cloud services. If you use a cloud service that is not on the [FedRAMP Marketplace](#), you will need to determine whether that service has in place security protections that are “equivalent” to those at the FedRAMP Moderate impact level. Unfortunately, there are no official definitions for how to determine FedRAMP equivalency.

The CMMC Information Institute recommends that the cloud service provider obtain a letter of attestation from an authorized [FedRAMP 3rd Party Assessment Organization](#) (“**FedRAMP 3PAO**”) which states that the FedRAMP 3PAO has reviewed the cloud service provider's “body of knowledge” and that the FedRAMP 3PAO believes the cloud service would likely be awarded a FedRAMP ATO. If you are not able to obtain such a letter from the cloud service provider and they are not on the FedRAMP Marketplace, additional diligence should be conducted before you trust the cloud service provider with CUI.

2

Choose Your Tool

Choose Your Tool

After you have decided whether to get help or go it alone, the next step is to decide how you will collect and organize all of the evidence and other information you will need as part of the compliance program. There are a



wide range of options, from spreadsheets and file folders to databases to OneNote files to online tools like [FutureFeed](#). Each option has its own strengths and weaknesses.

For very small organizations, such as those with 1-5 employees, spreadsheets and file folders may be perfectly adequate. Those organizations will likely have only a handful of assets (i.e., people, equipment, locations, etc.) that are involved in the storage, processing (i.e., use), or transmission of the government's information. Using spreadsheets and file folders is advantageous because there are free spreadsheets available, such as the spreadsheet from the [CMMC Information Institute](#), which can help you along the way.

Organizations with more than a handful of employees and other assets will likely benefit from using a more robust tool, like the [FutureFeed](#) platform. These tools streamline and automate many of the functions described in the ten remaining steps below. Although there are fees associated with these services, they often accelerate the compliance process enough to pay for themselves in time saved.

3

Find the FCI and CUI

Find the FCI and CUI

At its core, CMMC is focused on ensuring that FCI and CUI are properly safeguarded. To understand whether you are properly safeguarding FCI and CUI, you need to know what FCI and CUI you have. This means that you need to conduct a basic information inventory.

That inventory should identify not only where the information currently resides, but also:

- where it came from (e.g., prime contractor, other contractor, government agency, etc.)
- how it entered the organization (e.g., removable media via mail/courier, E-mail attachment, secure file transfer, etc.)

- in what form(s) it is stored, processed, or transmitted (e.g., paper, E-mail, encrypted file on removable media, etc.)
- how it moves through the organization (i.e., who accesses the information, and why)
- how it leaves the organization (e.g., removable media, E-mail, secure file transfer, etc.)

While you are at it, you should look not only for FCI and CUI in your environment, but also for other forms of sensitive or regulated information. This includes, for example, personnel records, payment card information, healthcare records, student information, client information, intellectual property from your business partners and vendors, and your company's own intellectual property.

If you do have some of these other forms of commercially sensitive information, you should catalog the safeguarding requirements associated with that information. For example, if you received intellectual property as part of a business relationship with another organization, your contract with that organization probably also imposes certain safeguarding requirements on you with respect to that information. Similarly, if you handle credit card information, you may be subject to the **Payment Card Information ("PCI")** standards.

This booklet focuses on compliance with the CMMC requirements. However, it will hopefully be apparent how these same concepts can be applied to compliance with other requirements, such as those described above.

4

Determine: CMMC
L1, L2, or L3?

Determine: CMMC Level 1, 2, or 3?

As a DoD contractor, you need to determine the requirements that must be included in your compliance program. The list of requirements will inherently include those in CMMC. If you only handle FCI, then you should only need to comply with the CMMC Level 1 requirements. If you



handle CUI, you must comply with not only the CMMC Level 1 requirements for your assets that handle FCI, but also the CMMC Level 2 requirements for your assets that handle CUI. DoD has not yet specified when CMMC Level 3 will be required.

If you handle CUI Specified, you will also need to comply with the requirements defined in the corresponding LRGWP.

In addition, you should be aware of the requirements in DFARS [252.204-7012\(c\)-\(g\)](#). These include incident reporting requirements, the use of only FedRAMP Authorized (or equivalent) cloud services, and more. While these requirements are technically not part of a CMMC assessment, they should still be tracked for compliance purposes.

5

Establish an SSP
Framework

Establish a System Security Plan ("SSP") Framework

Although not technically required in CMMC Level 1, it is a good practice to begin creating a **System Security Plan ("SSP")**. The SSP defines the requirements you need to meet and how you meet them.

If you are using a tool like [FutureFeed](#), this will likely be done automatically for you. If you are using a spreadsheet, some will help you create an SSP, and in other cases you will want to use an SSP template like the one [published by NIST](#).

Regardless of whether it is created automatically for you or if you have to create it yourself, the goal of the SSP is to create a structured cybersecurity program. The effort you put into it now will make your organization significantly more secure and will make maintaining that level of security much easier.

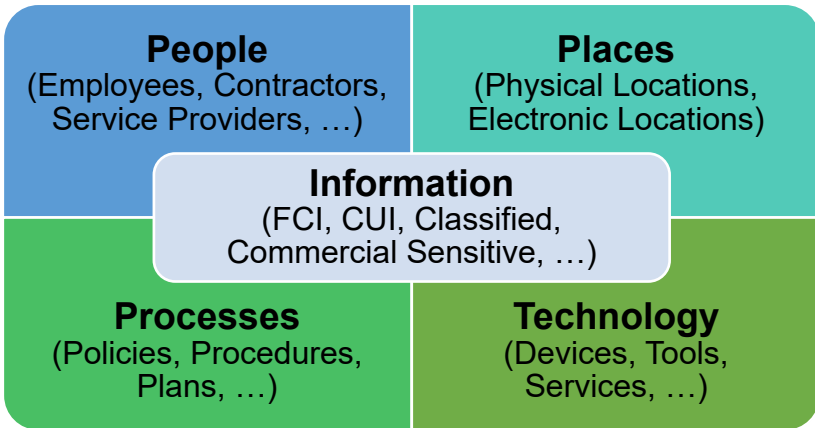
6

Inventory Your
Assets

Inventory Your Assets

In addition to the basic information inventory, when it comes to a CMMC assessment, you will also need to know:

- **People:** Who has access to the relevant FCI or CUI, and why do they need access?
- **Places:** Where is the FCI or CUI stored, processed, or transmitted (e.g., offices, data centers, etc.)?
- **Technology:** What hardware, software, and other technology is used to store, process, or transmit the FCI or CUI?
- **Processes:** What documentation (e.g., policies, procedures, plans, drawings, etc.) do you have that helps describe how you are safeguarding the FCI or CUI?



If you don't have any CUI but you would like to become a government contractor who is authorized to handle CUI, you should build your program based on the type(s) of CUI you expect to handle. Your prime contractor or a government representative, like a Contracting Officer or Program/Project Manager, can help you identify this.

7

Define Current and Desired Scope

Define Current and Desired Scope

Once you have completed the data inventory and identified the corresponding requirements, the next step is to determine the “scope” of the environment to be assessed. For many small businesses this will be the entire company's network. However, for companies with

more than 15-20 employees, it may be more economically efficient and secure to compartmentalize the government's information (especially CUI) into a secure "enclave," or separate IT environment.

The [CMMC Scoping Guides](#) have additional details on how to establish scope. In a nutshell, if the contractor is handling CUI and the contractor wants to position a piece of equipment, a person, a physical location, or another "asset" so that it is "out of scope" and not subject to the compliance requirements, the contractor must physically or logically isolate the assets that handle CUI from those which do not.

For example, in a building, this means that CUI must be stored, processed, or transmitted in rooms with appropriate physical access controls that prevent unauthorized persons from accessing the CUI. In a network, this means that equipment handling CUI must be on separate, dedicated VLANs, subnets, or networks so that only authorized equipment and users can access the CUI.

8

Identify Gaps and
Create POA&Ms

Identify Gaps and Create POA&Ms

Now that you know what is "in scope" for your compliance review, the next step is to compare your in-scope assets and information against the various requirements. When it comes to assessing CMMC compliance, be sure your assessment includes not only the requirements in [NIST SP 800-171](#), but also the objectives in [NIST SP 800-171A](#). In a platform like [FutureFeed](#), this is handled automatically for you. Some spreadsheets and other free resources that are available online only help you track compliance at the requirement level, which is not sufficient for CMMC certification purposes.

The goal of this "gap assessment" is to identify the gaps between what you are doing now and what you are expected to do under

the corresponding law, regulation, government-wide policy, contractual requirement, etc. At this stage, it is important to be honest and self-critical as you evaluate your compliance. When in doubt, you should err on the side of marking yourself as noncompliant.

At the same time, be sure to not dwell on things that are missing. If a gap is identified, simply make a record of the gap and move on. Don't bother trying to remediate things, even if it is only the creation of a minor piece of documentation, at this stage of the game. Most companies identify between 150 and 250 gaps in their programs when they conduct their first gap analysis. If you are like them, you will probably make significant changes to your information security program that may cause you to rethink things anyway, so these early remediation efforts will probably be of limited value.

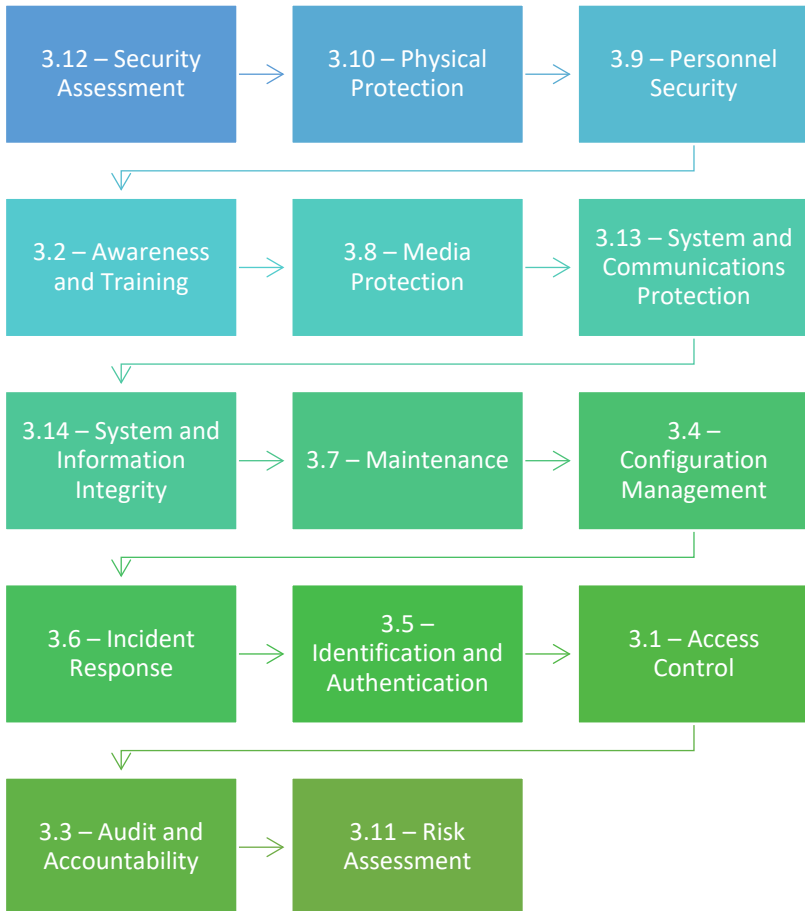
If your organization meets a particular requirement, you should record that fact in the SSP, including a description of how the organization meets the requirement. If you have evidence, such as policies, drawings, screen captures, log files, etc. that help prove that the requirement is met, they should be noted in the SSP as well. This builds a "traceability matrix" that allows any third-party, such as an assessor or auditor, to understand the organization's compliance with the requirements.

Without the traceability matrix, the assessor would, in theory, have to comb through every document you create trying to find the needle in the haystack that proves your compliance. Most assessors won't spend that much time on your assessment; they will likely fail you instead. We will talk about evidence in more detail in steps 9 and 10.

If you are not familiar with [NIST SP 800-171](#) or CMMC, we recommend that you do not conduct your gap assessment in the order in which the requirements appear in those documents. This is because, quite frankly, some of the requirements in the Access



Control family can be difficult to understand. Starting with them can make the process feel daunting and be discouraging. Instead, we recommend working through the domains in the following order:



With a good sense for the gaps in your information security program, the next step is to create a remediation plan. To do this, you should create a **Plan of Action & Milestone(s)** (“**POA&M**”), for each gap you identified. The POA&M should include:

- a description of what needs to be done (your “plan of action”),

- one or more milestones that align with the plan of action,
- the person/people who will be involved in closing the POA&M, and
- financial commitments from the company to ensure that the POA&M is closed.

In many cases, since the remediation of one gap may allow another to also be remediated, it may be more efficient to group the POA&Ms into projects. Grouping POA&Ms into projects also makes it easier to prioritize the remediation activities and manage the remediation process. It also makes it much easier for management to oversee the remediation process.

9

Close POA&Ms

Close POA&Ms

After the POA&Ms and projects are created, the next step is to begin the remediation process. As you remediate, your goal should be to not only meet the requirement, but also to document the practice(s) implemented by your organization that allow it to meet the requirement.

In general, practices are comprised of policies, procedures, plans, and the corresponding evidence. It is helpful to understand the differences between these types of documents.

- **Policies** are high-level statements that describe how the organization intends to meet a particular requirement. For example, an employee off boarding policy might include language like: “All accounts associated with a terminated employee must be disabled within four (4) hours of the employee’s termination. The Director of HR shall notify the CISO as promptly as possible, and not more than thirty (30) minutes, after the termination of an individual’s employment with the company. The CISO shall ensure that all accounts associated with the terminated employee are deactivated



within three (3) hours of receipt of the termination notification from the Director of HR.”

- **Procedures** are step-by-step instructions that guide the responsible party through the process of meeting the company’s intent as described in a policy. For example, an employee off boarding procedure may include instructions which guide a system administrator through the process of logging into Microsoft 365 and deactivating a terminated employee’s account, and how to report the completion of that process to the CISO. In some cases, several procedures might be required to comply with a single policy. When writing procedures, your goal should be to write them with sufficient detail that junior-level employees can follow them wherever possible.
- **Plans** are similar to procedures, except that they require the person following them to make one or more decisions while following the plan. For example, an incident response plan may require the person executing the plan to decide whether a particular event is significant enough that it must be reported to law enforcement and regulators, or whether to shut down the company’s entire IT systems. Since these decisions can have significant consequences for the organization, the execution of a plan is often reserved for management-level employees.
- **Evidence** demonstrates that the policies, procedures, and plans are followed as part of the organization’s normal course of business. If the organization does not collect evidence, proving compliance with the organization’s policies, as well as the broader legal and regulatory requirements the policies address, will be exceedingly difficult. Evidence can take many forms, including screen captures of system configurations and worksheets that are signed off by the responsible employee which document the steps taken by the employee.

Assessment teams are generally looking for three types of evidence: Examine, Interview, and Test. While the assessment team may not request every type of evidence for every requirement, your implementation team should be prepared to offer all three types wherever practical and relevant.

- **Examine** – This is comprised of documents that can be reviewed as part of the early phases of the assessment. The assessment team will review the documents to understand the scope of the assessment and how the organization expects to meet the various requirements.
- **Interview** – Once the assessment team has reviewed the documentation, they will interview members of your organization (including your IT or security service providers, where applicable). The goal of the interview is to ensure that the day-to-day work that is performed is consistent with the documentation. For example, if the organization's password policy requires all passwords to be at least 12 characters long and, during the interview, a member of your team who is responsible for configuring password policies says that passwords need only be 8 characters long, that could create issues.
- **Test** – Assuming the documentation and interview are in alignment, the assessment team may also ask your team to demonstrate how the requirement is met in your live environment. For example, you may be asked to open Microsoft 365 and to prove that the password complexity settings are consistent with the policy.

As noted above, the SSP should also include a traceability matrix. A traceability matrix helps the assessment team easily identify which practices your organization considers relevant for a particular requirement. This allows the assessment team to more easily review the practices to ensure they align with the requirements.

10

Validate

Validate

With the gaps closed and a comprehensive program in place, it might seem as though it is time to call in a C3PAO to assess your organization. However, we recommend making one more pass through the SSP and requirements. We're all human, and often mistakes are made, or actions are taken that were only meant to be temporary but then are forgotten about. Making one last "validation" pass through the requirements help ensure all the "i"s are dotted and "t"s are crossed before you engage the third-party assessment organization.

11

Certify

Certify

The next step in this process is to engage a C3PAO to conduct a formal assessment of your compliance with the requirements. Be sure to only select a C3PAO who is currently listed in the [Cyber AB's Marketplace](#).

If the assessment is successful, the C3PAO will issue a certificate of compliance to you and record that certificate with DoD.

12

Maintain

Maintain

The last step in the process is to maintain your environment's compliance with the requirements. As noted above, although CMMC certifications are valid for three years, contractors must self-certify their continued compliance in the off years.

Why should I use a tool like FutureFeed as Part of My Compliance Program?

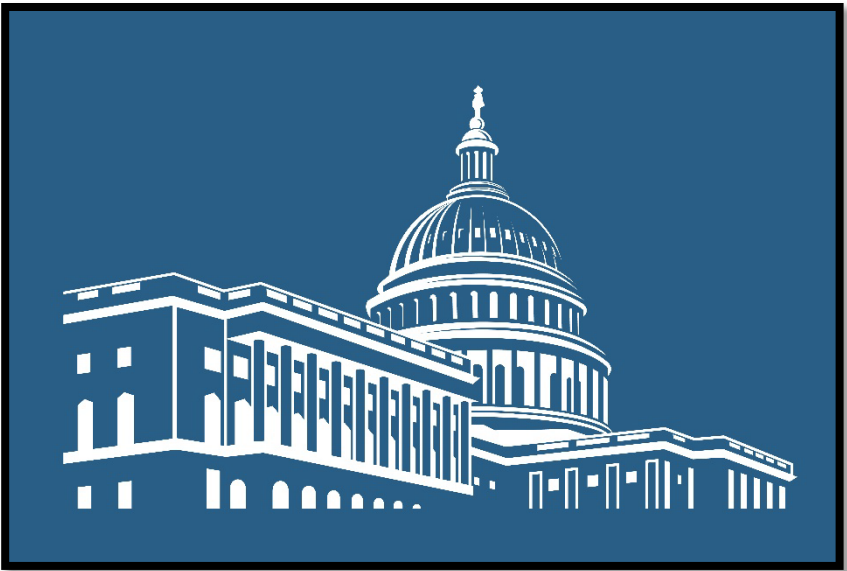
You can conduct, store, and maintain your information and other inventories directly in the [FutureFeed](#) platform. Unlike spreadsheet-based tools, [FutureFeed](#) automatically builds your SSP and POA&Ms for you as you conduct the gap assessment.

You can use the built-in project management capabilities to track the completion of POA&Ms and projects.

As you work, the [FutureFeed](#) platform calculates your SPRS score in real time, and the automated dashboards and deliverables make it easy for everyone to track the organization's progress. [FutureFeed](#) also allows you to easily organize and store your evidence, including new evidence and evidence of continuous compliance.

In short, [FutureFeed](#) accelerates the creation of your CMMC compliance program. Visit <https://FutureFeed.co> for more information and to schedule a demonstration!

Official Federal Resources



NIST FRAMEWORK DOCUMENTATION

SP 800-171 r2

800-171 - Framework including controls

<https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final>

800-171A - Assessment Guide

<https://csrc.nist.gov/pubs/sp/800/171/a/final>

SP 800-171 r3 DRAFT

Framework including controls – Final Public Draft

<https://csrc.nist.gov/pubs/sp/800/171/r3/fpd>

Assessment Guide - Initial Public Draft

<https://csrc.nist.gov/pubs/sp/800/171/a/r3/ipd>

SP 800-172

Enhanced security requirements. Likely pre-cursor to CMMC Level 3.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf>

CUI DOCUMENTATION

NARA CUI Registry

Categories of CUI across-government

<https://archives.gov/CUI/registry/category-list>

DoD CUI Registry

DoD-specific CUI Categories

<https://www.dodcui.mil/>

NARA CUI Marking Handbook

Official methods for marking CUI

<https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf>

FCI DOCUMENTATION

FAR 52.204-21

FCI – Security requirements to safeguard non-public federal contract information.

<https://www.acquisition.gov/far/52.204-21>

PROCUREMENT REGULATION AND DOCUMENTATION

CMMC Model, Scoping Guide, and Related Documents

Official CMMC DoD Materials

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

DoD Procurement Toolbox Cybersecurity FAQs

Expectations from the perspective of the contracting officer.

<https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2022-12/Cybersecurity%20FAQ%20update%2012-19-22.pdf>

DoD Instruction 5230.24

DoD Distribution Statements – Everything you need know

<https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/523024p.pdf>

DFARS 252.204-7012

Primary regulation for Covered Defense Information and Cyber Incident Reporting. Clauses (c)-(g) include requirements going beyond CMMC.

<https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>.

DFARS 252.204-7019

Notice of DoD Cyber-Assessment Requirements to be considered for award.

<https://www.acquisition.gov/dfars/252.204-7019-notice-nist-sp-800-171-dod-assessment-requirements>.

DFARS 252.204-7020

Requires contractors to provide the Government with access.

<https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171-dod-assessment-requirements>.

DFARS 252.204-7021

CMMC-Specific DoD Cyber-Assessment Requirements

<https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements>.

DFARS 252.204-7024

Regulation re: the use of the SPRS Score in contract decisions.

<https://www.acquisition.gov/dfars/252.204-7024-notice-use-supplier-performance-risk-system>.

SPRS Factsheet

Basic expectations and explanation of SPRS

https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/SPRS_FactSheet.pdf

Key CMMC



Advisory and Training Resources

***NIST Manufacturing Extension Partnerships**

Assistance to manufacturers. May include financial and advisory resources.

<https://www.nist.gov/mep/cybersecurity-resources-manufacturers>

***APEX Accelerators**

(formerly the Procurement Technical Assistance Program)

Assistance to manufacturers. May include financial and advisory resources.

<https://www.apexaccelerators.us/>

***United States Air Force Blue Cyber Education Series for Small Business**

<https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/>

Mandatory DoD CUI Training

This course is mandatory training for all DoD personnel with access to controlled unclassified information.

<https://securityawareness.usalearning.gov/cui/index.html>

Project Spectrum

Free government-backed website with very basic CMMC compliance training and tools.

<https://www.projectspectrum.io/#/>

CCP and CCA Licensed Training Provider

SMU offers both CCP and CCA programs as a CAICO LTP.

CCP: <https://www.smu.edu/CAPE/Programs/Certificates/CCP>

CCA: <https://www.smu.edu/CAPE/Programs/Certificates/CCA>

The CMMC Information Institute

Non-profit resource with up-to-the minute definitive information regarding CMMC, CUI, and more.

<https://CMMCInfo.org>

15 Minutes with FutureFeed

No cost resource available weekly to provide answers regarding CMMC implementation from Cyber AB certified professionals.

<https://FutureFeed.co/15>

* May have financial resources available depending upon state and business standing.

CMMC Official Resources

The Cyber AB

The accreditation body for CMMC. Definitive information about the assessment process and the training and certification programs that support it.

<https://CyberAB.org>

Cyber AB – Licensed Training Providers

Find an officially licensed training provider for staff certifications.

<https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending?typeld=10>

SMU LTP Listing:

<https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending?term=southern%20methodist%20university>

Cyber AB – Official C3PAO (Assessment Organization) Listing

Find a list of authorized C3PAOs to conduct an official assessment.

<https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending?typeld=7>

Cyber AB – Registered Provider Organizations (“RPOs”)

Find a list of organizations which have committed significant resources to participate in the CMMC ecosystem and which can help you create your CMMC compliance program.

<https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending?typeld=3>

Government Reporting Requirements

DoD Cyber Crime Center (“DC3”) Defense Industrial Base (“DIB”) Cybersecurity Program

DCISE is the operational hub of the Defense Industrial Base (DIB) Cybersecurity Program of the Department of Defense, focused on protecting intellectual property and safeguarding DoD content residing on, or transiting through, contractor unclassified networks.

<https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/>

DIBNet Portal

Mandatory portal to report cyber-incidents. Registration, approval, and certificates issued in advance required for use.

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

SPRS Portal

Report NIST SP 800-171 compliance scores on this site, operated by the Navy, and often required to qualify for contracts and to operate as a

subcontractor for DoD contracts that include a DFARS clause.
Registration and approval required for use.
<https://www.sprs.csd.disa.mil/>

Tools and Financial Services

FutureFeed

Leading Cyber-GRC platform, focused on NIST SP 800-171 / CMMC Compliance. Micro-training and starter templates built-in.
<https://FutureFeed.co>

Parabilis

Working capital financing for government contractors (especially with cyber-compliance funding needs).
<https://Parabilis.com>

CISA

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

Acronyms



Acronyms

3PAO	FedRAMP Authorized 3 rd Party Assessment Organization
ATO	Authorization to Operate
C3PAO	CMMC 3 rd Party Assessment Organization
CAGE	Commercial and Government Entity code
CCA	Certified CMMC Assessor
CCP	Certified CMMC Professional
CDI	Covered Defense Information
CFR	Code of Federal Regulations
CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulations Supplement
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	United States Department of Defense
DoJ	United States Department of Justice
FAR	Federal Acquisition Regulations
FCI	Federal Contract Information
FedRAMP	Federal Risk and Authorization Management Program
FOUO	For Official Use Only
ITAR	International Traffic in Arms Regulations
LRGWP	Law, Regulation, or Government-Wide Policy
LTP	Licensed Training Provider
NARA	National Archives and Records Administration
POA&M	Plan of Action and Milestone
RFI	Request for Information
RFP	Request for Proposal
RP	Registered Practitioner
RPO	Registered Provider Organization
SBU	Sensitive but Unclassified
SPRS	Supplier Performance Risk System
SSP	System Security Plan



 **FutureFeed**
Attain. Maintain. **Prove it Anytime.**