

October 8, 2024

# Regulatory Changes to CMMC & Impact to the DIB

BY JOY BELAND



# Joy Beland

Welcome!

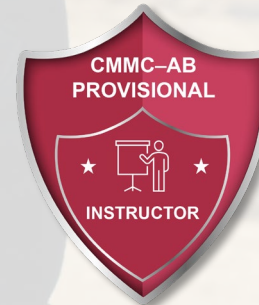


**Vice President, Cybersecurity Compliance**

**QTE | CISM | SSAP | CMMC CCA & PI**

310-590-9288; [Joy.beland@summit7.us](mailto:Joy.beland@summit7.us)

<https://www.linkedin.com/in/joy-belinda-beland>



# Agenda

A LOT OF GROUND TO COVER...

- 01** How We Got Here
- 02** CMMC Brief Overview
- 03** The SMB DIB Challenge
- 04** Shared Responsibilities
- 05** Resources





# How We Got Here

THE 1,000 FOOT VIEW

# How Did We Get Here?

The Speed of a Crawl

2001



2025

# Sensitivity of Shared Data

## FCI – Federal Contract Information

*Contracts issued by the acquisition team acting on behalf of the DoD.*  
“Information, not intended for public release, provided by, or generated for the Government under a contract to develop or deliver a product or service to the Government.”

## CUI – Controlled Unclassified Information

*Data generated under the contract or used to manufacture goods as part of a contract.*  
“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.”



# Which Supply Chains Process, Store or Transmit CUI?



Department of Defense



NASA



Department of Energy



Department of Agriculture



Department of Homeland Security



General Services Administration



Department of Commerce



Department of Treasury



Environmental Protection Agency



Department of Education  
(Federal Student Aid)



Nuclear Regulatory Commission



Department of Housing & Urban Development



Federal Energy Regulatory Commission

# Title 32 of the Code of Federal Regulations (C.F.R.)

## PART 2002 - CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Authority: 75 FR 68675, 3 CFR, 2010 Comp., pp. 267-270.

Source: 81 FR 63336, Sept. 14, 2016, unless otherwise noted.

### Subpart A - General Information

#### § 2002.1 Purpose and scope.

- (a) This part describes the executive branch's Controlled Unclassified Information (CUI) Program (the CUI Program) and establishes policy for designating, handling, and decontrolling information that qualifies as CUI.
- (b) The CUI Program standardizes the way the executive branch handles information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526, Classified National Security Information, December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011, et seq.), as amended.
- (c) All unclassified information throughout the executive branch that requires any safeguarding or dissemination control is CUI. Law, regulation (to include this part), or Government-wide policy must require or permit such controls. Agencies therefore may not implement safeguarding or dissemination controls for any unclassified information other than those controls consistent with the CUI Program.
- (d) Prior to the CUI Program, agencies often employed *ad hoc*, agency-specific policies, procedures, and markings to handle this information. This patchwork approach caused agencies to mark and handle information inconsistently, implement unclear or unnecessarily restrictive disseminating policies, and create obstacles to sharing information.
- (e) An executive branch-wide CUI policy balances the need to safeguard CUI with the public interest in sharing information appropriately and without unnecessary burdens.
- (f) This part applies to all executive branch agencies that designate or handle information that meets the standards for CUI. This part does not apply directly to non-executive branch entities, but it does apply indirectly to non-executive branch CUI recipients, through incorporation into agreements (see §§ 2002.4(c) and 2002.16(a) for more information).
- (g) This part rescinds Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556 (June 9, 2011).
- (h) This part creates no right or benefit, substantive or procedural, enforceable by law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

General Information

Key Elements of the CUI Program

CUI Program Management

## ENHANCED CONTENT - TABLE OF CONTENTS

▼ Part 2002	Controlled Unclassified Information (CUI)	2002.1 – 2002.56
▼ Subpart A	General Information	2002.1 – 2002.8
§ 2002.1	Purpose and scope.	
§ 2002.2	Incorporation by reference.	
§ 2002.4	Definitions.	
§ 2002.6	CUI Executive Agent (EA).	
§ 2002.8	Roles and responsibilities.	
▼ Subpart B	Key Elements of the CUI Program	2002.10 – 2002.24
§ 2002.10	The CUI Registry.	
§ 2002.12	CUI categories and subcategories.	
§ 2002.14	Safeguarding.	
§ 2002.16	Accessing and disseminating.	
§ 2002.18	Decontrolling.	
§ 2002.20	Marking.	
§ 2002.22	Limitations on applicability of agency CUI policies.	
§ 2002.24	Agency self-inspection program.	
▼ Subpart C	CUI Program Management	2002.30 – 2002.56
§ 2002.30	Education and training.	
§ 2002.32	CUI cover sheets.	
§ 2002.34	Transferring records.	
§ 2002.36	Legacy materials.	
§ 2002.38	Waivers of CUI requirements.	
§ 2002.44	CUI and disclosure statutes.	
§ 2002.46	CUI and the Privacy Act.	
§ 2002.48	CUI and the Administrative Procedure Act (APA).	
§ 2002.50	Challenges to designation of information as CUI.	
§ 2002.52	Dispute resolution for agencies.	
§ 2002.54	Misuse of CUI.	
§ 2002.56	Sanctions for misuse of CUI.	

### Appendix A to Part 2002

Acronyms



# Defense Federal Acquisition Regulation Supplement (DFARS) in Title 48 of the C.F.R

<https://www.ecfr.gov/current/title-48/chapter-2>

ECFR CONTENT	
▼ <b>Title 48</b> Federal Acquisition Regulations System	Part / Section
▼ <b>Chapter 2</b> Defense Acquisition Regulations System, Department of Defense	200 – 299
▼ <b>Subchapter A</b> General	200 – 204
<i>Part 200 [Reserved]</i>	
<b>Part 201</b> Federal Acquisition Regulations System	201.101 – 201.670
<b>Part 202</b> Definitions of Words and Terms	202.101
<b>Part 203</b> Improper Business Practices and Personal Conflicts of Interest	203.070 – 203.1004
<b>Part 204</b> Administrative and Information Matters	204.101 – 204.7503
▶ <b>Subchapter B</b> Acquisition Planning	205 – 212
▶ <b>Subchapter C</b> Contracting Methods and Contract Types	213 – 218
▶ <b>Subchapter D</b> Socioeconomic Programs	219 – 226
▶ <b>Subchapter E</b> General Contracting Requirements	227 – 233
▶ <b>Subchapter F</b> Special Categories of Contracting	234 – 241
▶ <b>Subchapter G</b> Contract Management	242 – 251
▶ <b>Subchapter H</b> Clauses and Forms	252 – 253
<b>Part 252</b> Solicitation Provisions and Contract Clauses	252.101 – 252.251-7001
<b>Part 253</b> Forms	253.208 – 253.303
▶ <b>Subchapter I</b> Agency Supplementary Regulations	254
<i>Parts 254-299 [Reserved]</i>	
<b>Appendix A to Chapter 2</b>	
Armed Services Board of Contract Appeals	
<i>Appendixes B-E to Chapter 2 [Reserved]</i>	
<b>Appendix F to Chapter 2</b>	
Material Inspection and Receiving Report	
<i>Appendix G to Chapter 2 [Reserved]</i>	
<b>Appendix H to Chapter 2</b>	
Debarment and Suspension Procedures	
<b>Appendix I to Chapter 2</b>	
Policy and Procedures for the DoD Pilot Mentor-Protégé Program	

Purchasing vehicle: 252.204-7012 Which goes into all solicitations (RFP's and/or contracts) where CUI will be generated or shared.

# DFARS Clause 252.204-7012; Safeguarding Covered Defense Information And Cyber Incident Reporting

## What is it?

Amended in 2016 to provide for safeguarding of CUI when being stored, processed, or transmitted through a contractor's internal information system or network



## Requirements

Implement the controls within NIST SP 800-171 by Dec 31, 2017

If CUI is processed, stored or transmitted via cloud, it must be "Authorized" at FedRAMP Moderate or High (Government Cloud)

Report cyber incidents within 72 hours of discovery


Submit malicious software

Facilitate damage assessment



# DFARS 252.204-7012

## DIBCAC Assessment Results



**How many passed?  
Zero. Zip. Nada.**

**No skin in the game =  
No compliance**

# DFARS Family of Interim Rules

***Regulation (DFARS 252.204-7012) - based on trust by adding a verification component with respect to cybersecurity requirements***

## **DFARS clause 252.204-7019**

***Notice of NIST SP 800-171 DoD Assessment Requirements***

Called for the formal reporting of the **SPRS score** based on the weighted methodology to reflect current adherence to NIST 800-171 controls by Dec 31, 2017

## **DFARS clause 252.204-7020**

***NIST SP 800-171 DoD Assessment Requirements***

Requires a contractor to provide the **Government with access to its facilities; covers subcontractors as well**

## **DFARS clause 252.204-7021**

***Cybersecurity Maturity Model Certification Requirements***

**Introduces CMMC model & gives 2025 deadline**



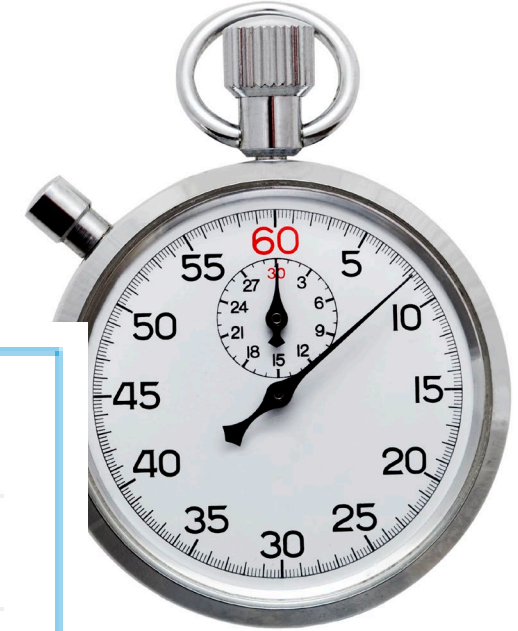
# How Did We Get Here?

The Speed of a Crawl



# What is Happening in the DIB – NOW?

SMB's in the Supply Chain



Source: RSAC Transforming 3<sup>rd</sup> Party Risk Management Executive Summary, Oct 2023

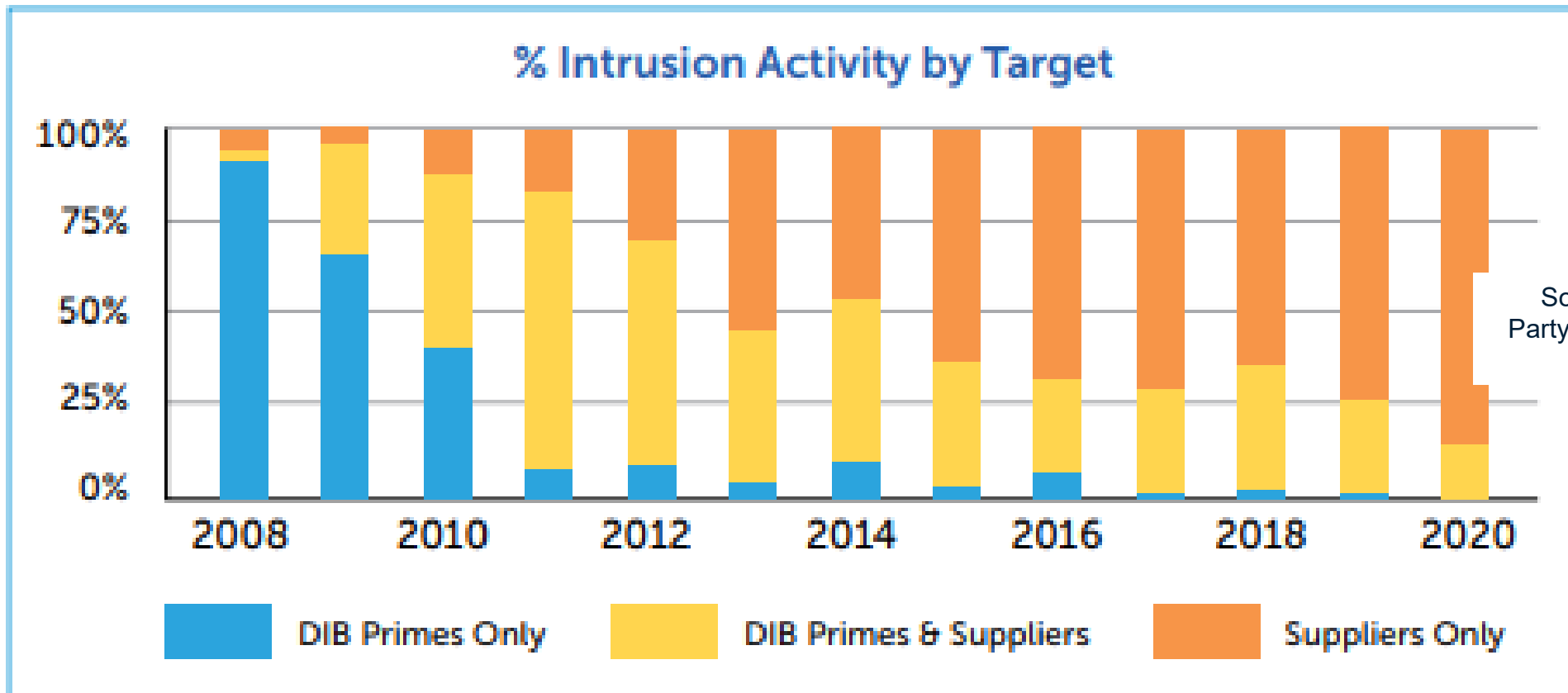


Figure 1: According to U.S. defense industry internal research, attackers have moved from targeting Defense Industrial Base prime contractors (DIB Primes) to suppliers. Similar trends have been seen in all sectors.







# CMMC Brief Overview

CMMC is NOT the requirements. CMMC is the program that assesses the requirements.

# NIST 800-171 – Required Controls to be Implemented

Domain	Level 1 Controls	Level 2 Controls	Grand Total
Access Control	4	18	22
Audit & Accountability		9	9
Awareness & Training		3	3
Configuration Management		9	9
Identification & Authentication	2	9	11
Incident Response		3	3
Maintenance		6	6
Media Protection	1	8	9
Personnel Security		2	2
Physical Protection	4	2	6
Risk Assessment		3	3
Security Assessment		4	4
System and Communications Protection	2	14	16
System and Information Integrity	4	3	7
<b>All Domains</b>	<b>17</b>	<b>93</b>	<b>110</b>



# Applicable to: Asset Category CUI

CUI Assets process, store, or transmit CUI as follows:

- **Process** – CUI can be used by an asset (e.g., accessed, entered, edited, generated, manipulated, or printed).
- **Store** – CUI is inactive or at rest on an asset (e.g., located on electronic media, in system component memory, or in physical format such as paper documents).
- **Transmit** – CUI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).

CUI Assets are part of the CMMC Assessment Scope and are assessed against applicable CMMC practices. In addition, the contractor is required to:

- document these assets in asset inventory;
- document these assets in the SSP; and
- provide a network diagram of the assessment scope (to include these assets) to facilitate scoping discussions during the pre-assessment.



# CMMC Will Impact: Everything in Scope

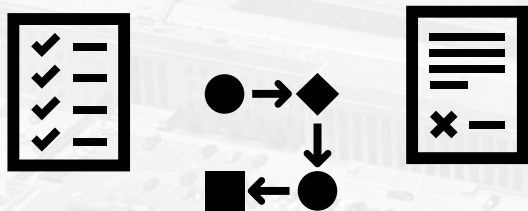
## People



## Technology



## Process



## Facility





An aerial photograph of a city, showing a grid of streets, buildings, and parking lots. A white rectangular box is overlaid on the right side of the image, containing the main title and subtitle. A vertical red bar is positioned to the left of the title text.

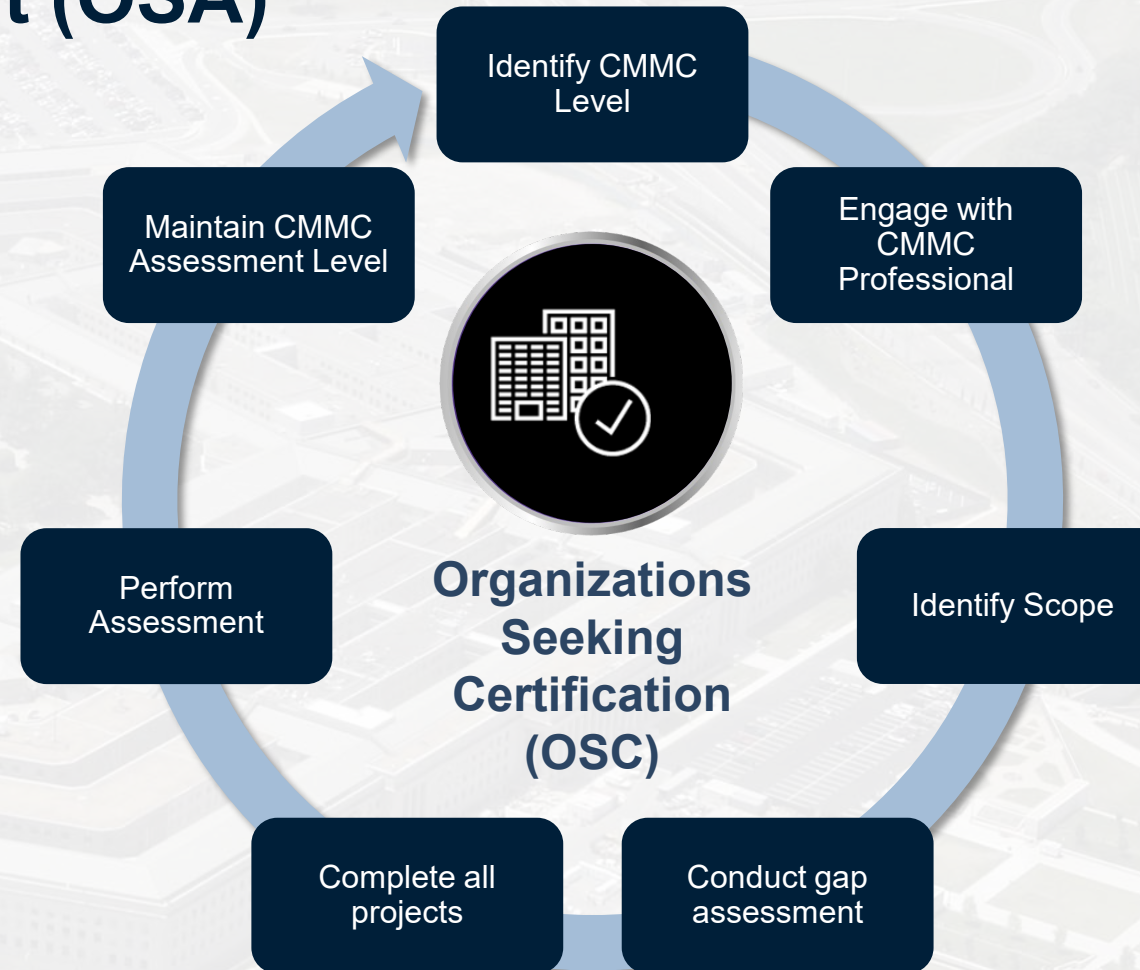
# The SMB/DIB Challenge

NO MAGIC BULLET



# Organizations Seeking Certification (OSC) Organizations Seeking Assessment (OSA)

**Average time for  
implementation:  
18-24 months**



# The DoD **CMMC** Timeline

## CMMC 2.0

2020

2021

**CMMC 2.0**

2022

**AUG 2022:**  
VOLUNTARY CMMC  
ASSESSMENTS  
STARTED

2023

**DEC 2023:**

**CMMC  
PUBLISHED** !

2024

**JAN 2025:**

**CMMC  
Certifications  
Start**

2025

# Consequences of Non-Compliance

## Failure to comply results in the loss of a contract

CMMC compliance (i.e., certification) is required at the time of award of a contract and must be checked by the contracting officer within the SPRS system prior to any award or other contract action.

## Contractual Liability

DFARS 7012 requires that “the contractor shall, prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 1 year for self-attestation or 3 years for L2 formal certification) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.”

## False Claims Act

False Claims Act (FCA), 31 U.S.C. §§ 3729 – 3733 is a federal statute originally enacted in 1863 in response to defense contractor fraud during the American Civil War. The FCA provided that any person who knowingly submitted false claims to the government was liable for double the government’s damages plus a penalty of \$2,000 for each false claim.

The FCA has been amended several times and now provides that **violators are liable for treble damages plus a penalty linked to inflation.**



An aerial photograph of a city, showing a grid of streets, buildings, and parking lots. A white rectangular box is overlaid on the right side of the image, containing text. A vertical red bar is positioned to the left of the text box.

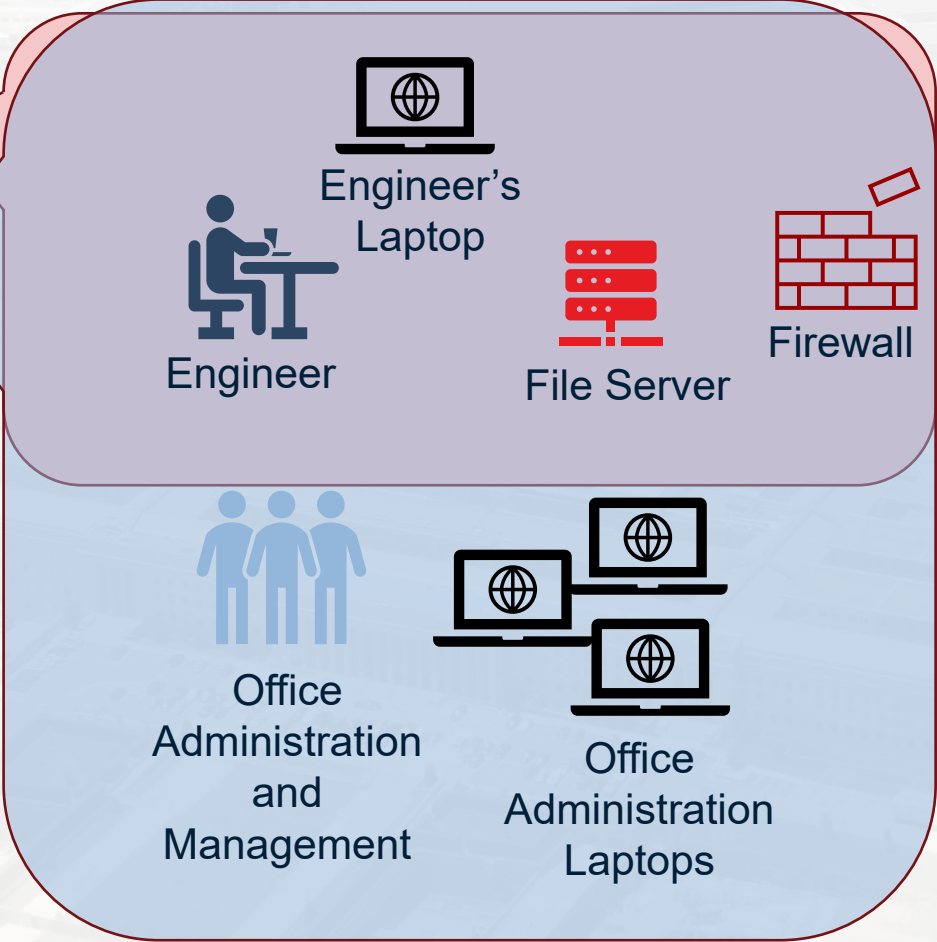
# Shared Responsibilities

WHERE SERVICES AND LIABILITY START & END

# External Service Providers: MSP (Managed Service Provider)

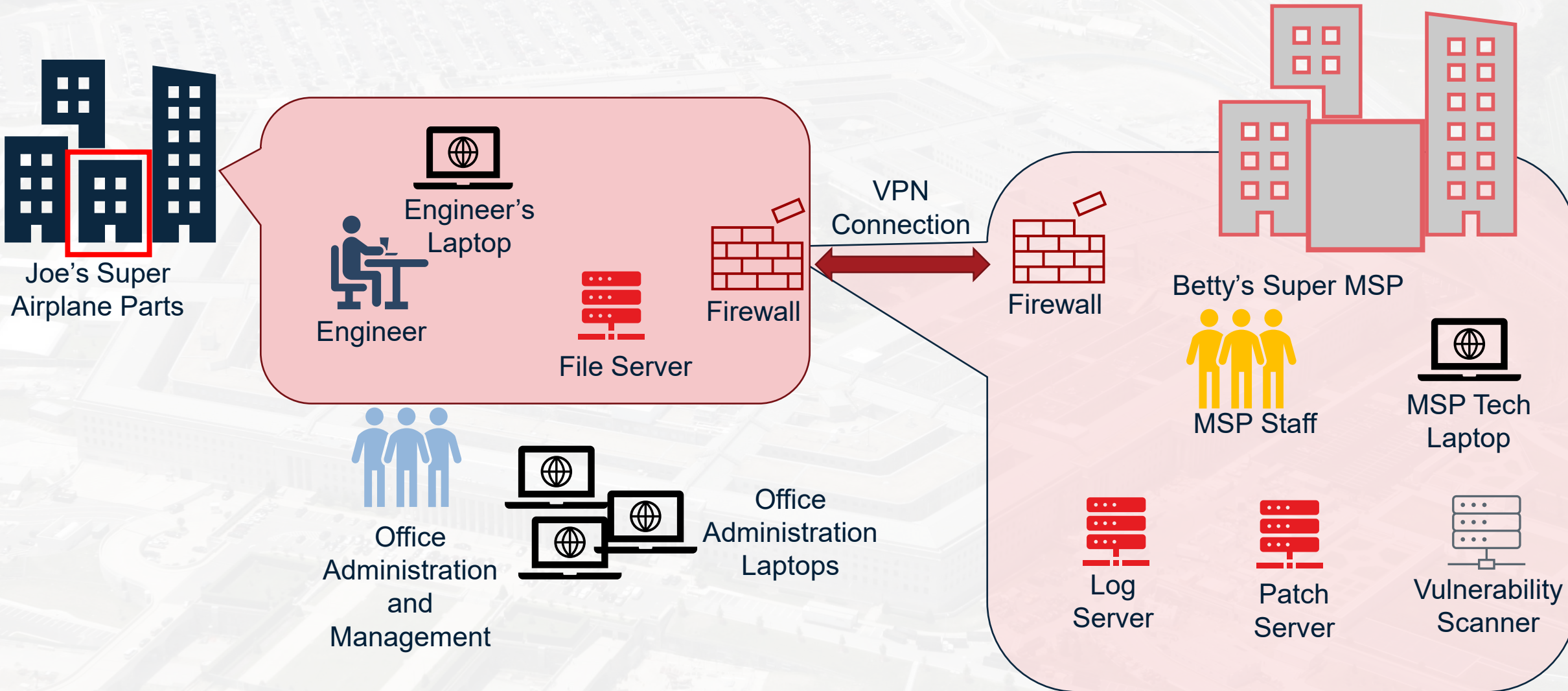


Joe's Super Airplane Parts





# External Service Providers: MSP (Managed Service Provider)





# External Service Providers: MSSP (Managed Security Service Provider)

## All Clear MSSP



Identity & Password Management





# CMMC Control “Inheritance”

A contractor can inherit practice objectives. A practice objective that is inherited is MET if adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective. An ESP may be external people, technology, or facilities that the contractor uses, including cloud service providers, managed service providers, managed security service providers, cybersecurity-as-a-service providers.

Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the assessment objectives are met. For each practice objective that is inherited, the Certified Assessor includes statements that indicate how they were evaluated and from whom they are inherited. If the contractor cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the contractor will receive a NOT MET for the practice.

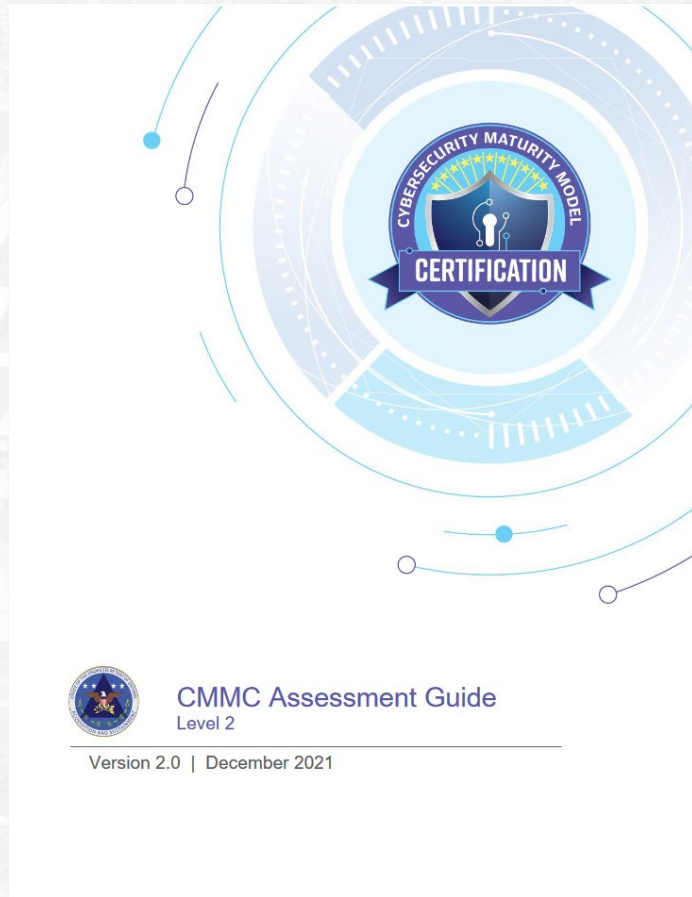


CMMC Assessment Score  
Level 2

Version 2.0 | December 2021



# The Ability to Achieve CMMC Certification Hinges Directly on the Quality of the Shared Responsibility Matrix



## External Service Provider Considerations

An ESP can be within the scope of applicable CMMC practices if it meets CUI asset criteria. Special considerations for a contractor using an ESP include the following:

- Evaluate the ESP's shared responsibility matrix where the provider identifies security control objectives that are the provider's responsibility and security control objectives that are the contractor's responsibility. In some instances, cloud service providers might expose configuration settings and parameters that the consumer can use to meet CMMC practice objectives.
- Consider the standards that the ESP conforms to and/or what accreditations it has (e.g., FedRAMP, SOC 2, and CMMC Certification).
- Consider the agreements in place with the ESP, such as service-level agreements, memoranda of understanding, and contracts that support the contractor's information security objectives.



# Shared Responsibility Matrix - Access Control Level 2 - 3.1.3



## AC.L2-3.1.3

Control the flow of CUI in accordance with approved authorizations.

**3.1.3 [a]** information flow control policies are defined.

**3.1.3 [b]** methods and enforcement mechanisms for controlling the flow of CUI are defined.

**3.1.3 [c]** designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.

**3.1.3 [d]** authorizations for controlling the flow of CUI are defined.

**3.1.3 [e]** approved authorizations for controlling the flow of CUI are enforced.

# Most Important Questions When Selecting a Service Provider

- Is the MSP focused on the DIB as their largest vertical?
- What is the MSP's current NIST SP 800-171A score?
- When is the MSP going to be ready for their own CMMC L2 assessment?
- Does the MSP employ individuals that are accredited as CCPs, CCAs, or RPAs? (RP is not a proof of knowledge)
- Does the MSP have a SRM they can share with you?
- Does the MSP include the SRM in their contract?



An aerial photograph of a university campus, showing various buildings, parking lots, and roads. The image is overlaid with a semi-transparent dark blue filter. A white rectangular box is positioned in the center-right of the image, containing the text. A vertical red bar is located on the left side of the white box.

# Resources

DON'T GO IN ALONE!

# Plenty of Help Out There!

## Groups and Associations that are Worth Checking Out:

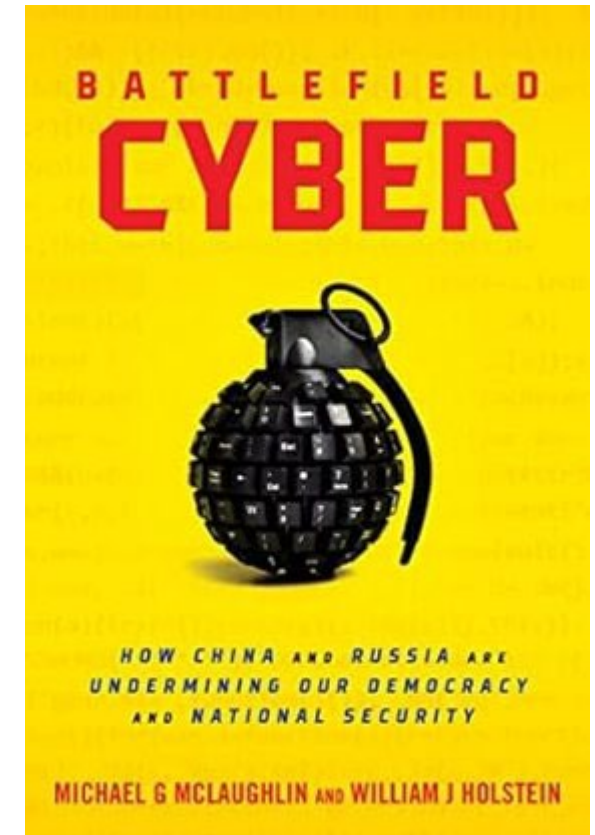
- <https://www.summit7.us>
- <https://www.mspscollective.org> – Industry Association of MSPs/ MSSPs dedicated to serving the Defense Industrial Base
- <https://cooey.life> – Discord Group
- <https://www.c3paoforum.org/> - Assessor Position Papers
- <https://www.cmmcaudit.org> – CMMC updates and resources

## People in the Know:

Jacob Horne, Caleb Leidy, Amira Armond, Scott Edwards, Carly Logan, Joy Beland, Jason Sproesser, Koren Wise, Allison Giddens - [LinkedIn](#)

## Training Resources:

- Edwards Performance Solutions – CCP and CCA classes
- GRC Academy
- Wise Technology

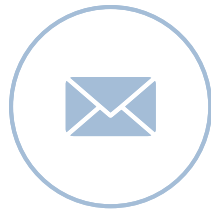




# Questions?



310.590.9288



[apex@summit7.us](mailto:apex@summit7.us)  
[Joy.beland@summit7.us](mailto:Joy.beland@summit7.us)



[info.summit7.us](http://info.summit7.us)