CMMC for MSPs:

The Opportunity and The Responsibility Workshop

February 4, 2026

MANAGED SERVICE PROVIDER COLLECTIVE

Introductions

Derek Kernus
Owner and CEO
Aethon Security

Joy Beland
VP Cybersecurity
Compliance Summit 7

Scott Edwards
CEO
Summit 7

MSP COLLECTIVE

AGENDA

1. The MSP Collective Intro
2. Why CMMC?
3. ESP Types
4. The Opportunity
5. Participation in Customer Assessments
6. Data types
7. The Scope
8. The Implementation
9. The SRM
10. The SSP
11. Q&A

Mission of MSPs for the Protection of Critical Infrastructure

Our Mission Statement

To inform the US Government and Critical Infrastructure industries on topics related to Managed Service Providers and Managed Security Service Providers dedicated to the National Security mission of maintaining a secure, functioning, and resilient critical infrastructure.

About Us

The MSP Collective is a nonprofit organization representing Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) dedicated to strengthening the cybersecurity posture of U.S. critical infrastructure. Founded in 2023, the Collective advocates for secure industry standards, informs government and industry leaders, and promotes the essential role of qualified, security-minded service providers in national cyber defense. Through initiatives like the External Service Provider (ESP) Directory, the MSP Collective connects critical infrastructure and Defense Industrial Base organizations with trusted, certified partners who meet the highest standards of reliability, compliance, and cybersecurity readiness.

MSP COLLECTIVE

History of the MSP Collective

- Stared in July of 2023 with Summit 7, NeoSystems & Quzara as the founding members
- Established as a 501(c)6 Non Profit Organization
- ISI joined in 2024 as a sustaining member

MSP COLLECTIVE

Board Members – 2 Year Terms

Terms Ending June 2026

- **Policy and Standards**
  - Derek Kernus, Aethon Security
- **Legislative Affairs**
  - Amy Edwards, Summit 7
- **Treasurer**
  - Bryan Champagne, ISI
- **Industry Relations**
  - Ed Bassett, NeoSystems
- **Operations**
  - Jason Sproesser, Summit 7

Terms Ending June 2027

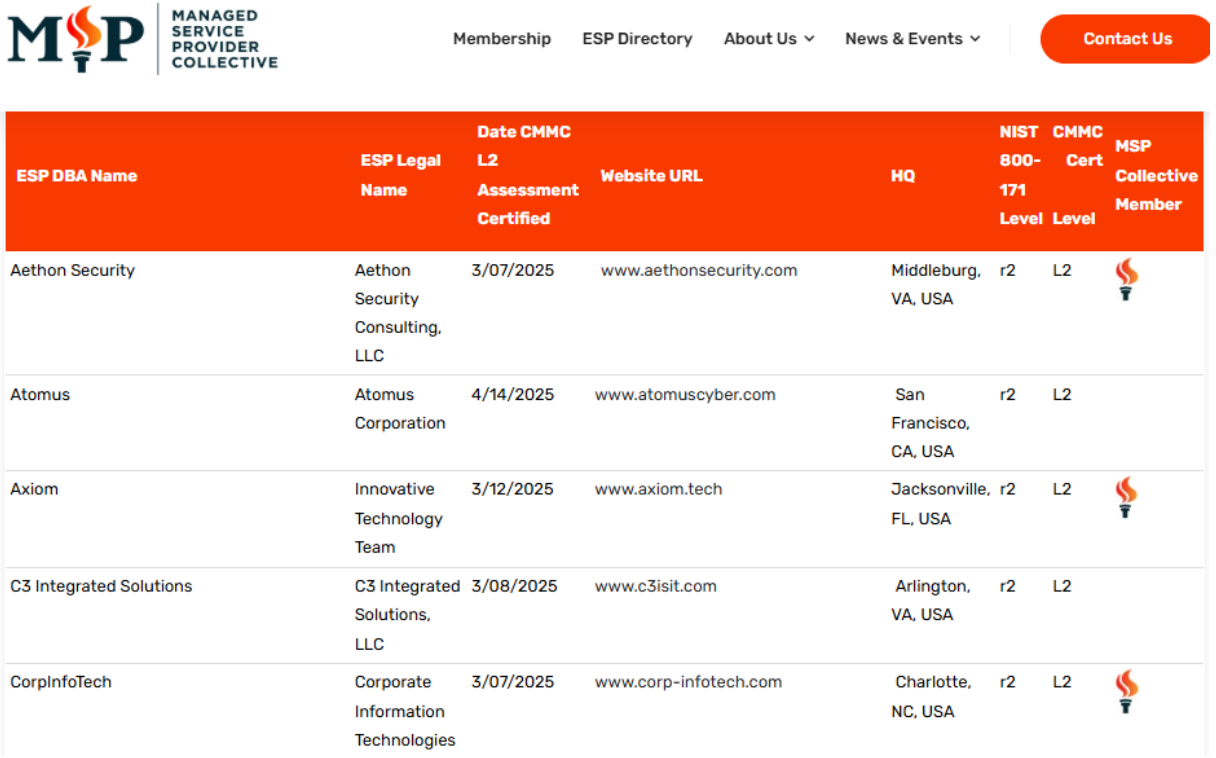
- **Executive Director**
  - Scott Edwards, Summit 7
- **Media Relations**
  - Megin Kennett, NeoSystems
- **EcoSystem Relations**
  - Joy Beland, Summit 7
- **Membership**
  - Open

MSP COLLECTIVE

The ESP Directory – 40+ MSPs/MSSPs

Requirements to be listed:

- Receive a CMMC Status of Final Level 2 (C3PAO) or Level 3 (DIBCAC)
- Ensure that your Scope includes the delivery infrastructure for your MSP / MSSP Services
- Ensure that your SRM is reviewed by the Assessing C3PAO



ESP DBA Name	ESP Legal Name	Date CMMC L2 Assessment Certified	Website URL	HQ	NIST 800-171 Level	CMMC Cert Level	MSP Collective Member
Aethon Security	Aethon Security Consulting, LLC	3/07/2025	www.aethonsecurity.com	Middleburg, VA, USA	r2	L2	
Atomus	Atomus Corporation	4/14/2025	www.atomuscyber.com	San Francisco, CA, USA	r2	L2	
Axiom	Innovative Technology Team	3/12/2025	www.axiom.tech	Jacksonville, FL, USA	r2	L2	
C3 Integrated Solutions	C3 Integrated Solutions, LLC	3/08/2025	www.c3isit.com	Arlington, VA, USA	r2	L2	
CorpInfoTech	Corporate Information Technologies	3/07/2025	www.corp-infotech.com	Charlotte, NC, USA	r2	L2	

MSP COLLECTIVE

Legislative Engagement

- MSP Certification
- MSP Regulation
- MSP Advocacy
- Government Education

- House and Senate Armed Services Committees
- Department of Defense
- CISA
- Other Federal Agencies
- State Legislatures
- Chambers of Commerce
- Cyber AB

MSP COLLECTIVE

Why CMMC?

What drove DoD to create this program?

MANAGED
SERVICE
PROVIDER
COLLECTIVE

We are in a Cyber War

China

- China has closed the technological gap with the United States in advanced weapon systems over the last 20 years. Much of this has happened via IP theft.

Critical Technologies

- According to the Australian Strategic Policy Institute, China now leads the United States in 66 of 74 critical technologies.
- Since 2020, China has surpassed the US in Small Satellites, Quantum Sensors, HPC, Advanced Integrated Circuits and Generative AI

According to the DoD, the DoD supply chain **loses ~$600,000,000,000** per year in IP to Cyber theft from China and other adversaries.

"The greatest wealth transfer in human history."

- Gen Keith Alexander, Former NSA Director

MSP COLLECTIVE

CUI Protection Rules and Laws

ITAR

1976: International Traffic in Arms Regulations

United States Munitions List (USML)

Designation & Sharing of CUI

May 2008: President Bush Memorandum

Executive Order 13556

November 2011: President Obama signs EO 13556 on CUI Protection

FedRAMP Policy

December 2011: FedRAMP Policy requiring CUI Protection in the Cloud

252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting

252.204-7019

Notice of NIST SP 800-171 DoD Assessment Requirements

252.204-7020

NIST SP.800-171 DoD Assessment Requirements

252.204-7021

Cybersecurity Maturity Model Certification Requirements

MSP COLLECTIVE

The CMMC Program Verifies if Contractual Cyber Requirements are Implemented

Prior to CMMC, Defense Contractors Simply Self-Attested Their Compliance

2013 — **2016** — **2020**

DFARS clause 252.204-7012 Created

- NIST SP 800-53 security requirements
- 72-hour incident reporting

DFARS clause 252.204-7012 Revised

- NIST SP 800-171 security requirements
- FedRAMP moderate or "equivalent"
- 72-hour incident reporting

FAR clause 52.204-21 Created

- 15 basic security requirements (FIPS 200)
- No incident reporting required

No 3rd-party verification required.
Must "flow down" to subcontractors.

DFARS clause 252.204-7021 Created

- "CMMC 1.0" maturity levels corresponded to the requirements in the FAR and DFARS
- Additional 20 requirements + "maturity processes"
- No "POAMs" or waivers

DFARS clause 252.204-7020 Created

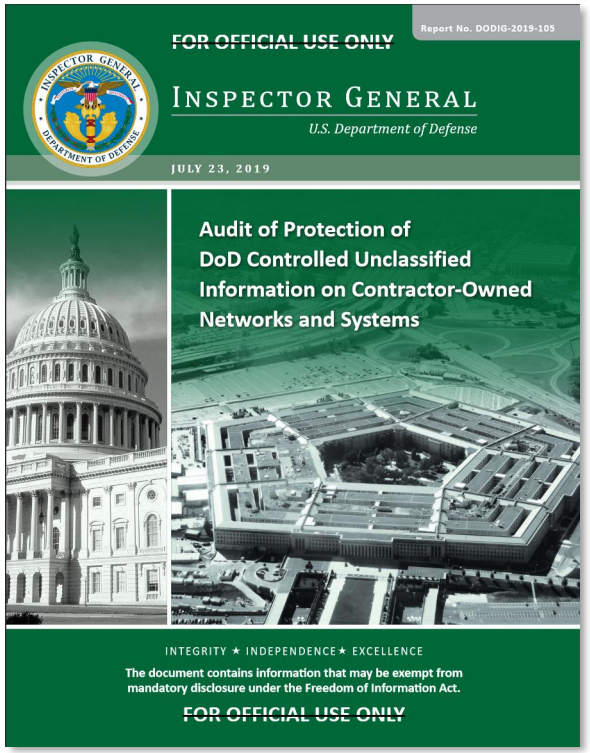
- Established standardized scoring system
- Must upload self-assessment score
- Allows DoD access to contractor systems for assessment

3rd-party verification required.
Must "flow down" to subcontractors.

MSP COLLECTIVE

DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information.

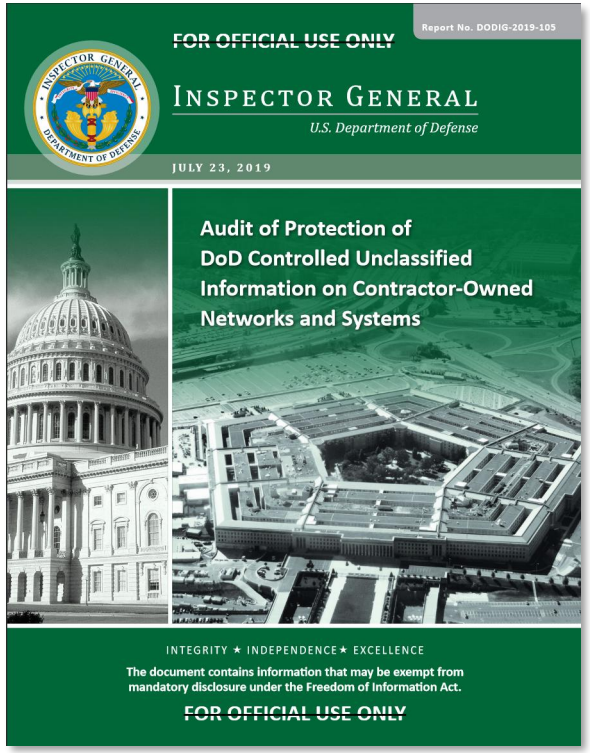
- Using multifactor authentication
- Enforcing the use of strong passwords
- Identifying network and system vulnerabilities
- Mitigating network and system vulnerabilities
- Protecting CUI stored on removable media
- Protecting CUI stored on removable media
- Overseeing network and boundary protection services provided by a third-party company
- Documenting and tracking cybersecurity incidents
- Configuring user accounts to lock automatically after extended periods and unsuccessful logon attempts
- Implementing physical security controls
- Creating and reviewing system activity reports
- Granting system access based on the user's assigned duties



2019

DoD Component contracting offices did not establish processes to:

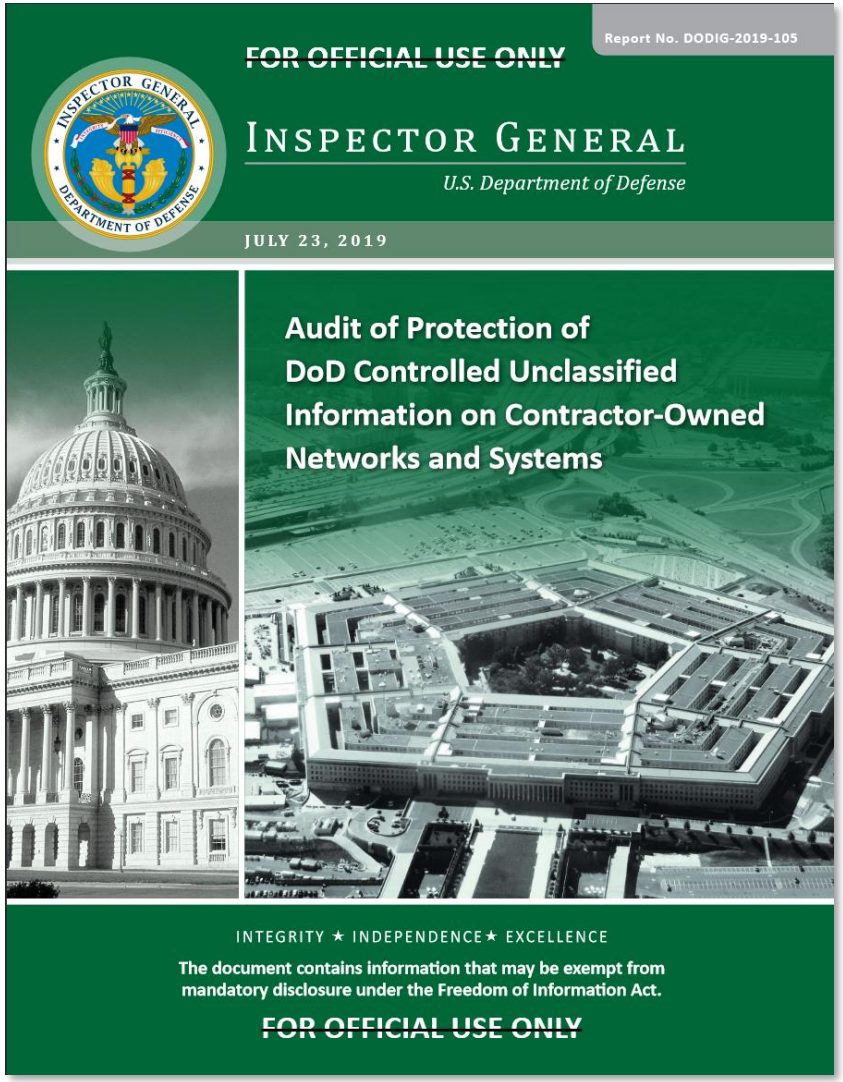
- Verify that contractors' networks and systems met [NIST] security requirements before contract award;
- Notify contractors of the specific CUI category related to the contract requirements;
- Determine whether contractors access, maintain, or develop CUI to meet contractual requirements;
- Mark documents that contained CUI and notify contractors when CUI was exchanged between DoD agencies and the contractor; and
- Verify that contractors implemented minimum security controls for protecting CUI



2019

MSP COLLECTIVE

As a result, the **DoD does not know the amount of DoD information managed by contractors** and cannot determine whether contractors are protecting unclassified DoD information from unauthorized disclosure. Without knowing which contractors maintain CUI on their networks and systems and taking actions to validate that contractors protect and secure DoD information, the **DoD is at greater risk of its CUI being compromised by cyberattacks from malicious actors who will target DoD contractors**.



2019

Voluntary CMMC assessments began December 2024

Mandatory CMMC assessments began November 2025 as part of the “phased roll-out”

2021

CMMC Program on “Strategic Pause”

- Self-attestation to FAR and DFARS cyber requirement still included in contracts
- DFARS clause 252.204-7020 **not paused**
- Still required to upload self-assessment scores

2024

CMMC Program Revised (32 CFR 170)

- Codified CMMC as Pentagon policy
- Streamlined to three levels
- Strictly aligned to NIST 171 and 172
- No maturity processes
- POAMs and waivers allowed (somewhat)

2025

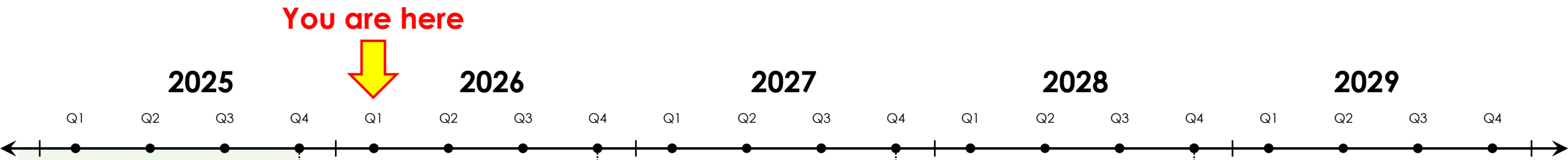
DFARS clause 252.204-7021 Revised

- Implemented CMMC policy in contracts
- Contracting officers indicate the level required
- Flows-down to subcontractors

MSP COLLECTIVE

CMMC status is a condition of contract award as of 11/10/25

CMMC phases do not prevent 3rd-party certification requirements (L2/L3) from showing up



"Market Roll-Out"

- **Began 12/16/2024**
- CMMC assessments commercially available

CMMC Phase 1

- **Began 11/10/2025**
- Level 1 & Level 2 (Self) in new solicitations & contracts
- In option periods for contracts awarded prior to Phase 1 at DoD discretion
- Level 2 (C3PAO) at DoD discretion

CMMC Phase 2

- **Begins 11/10/2026**
- Phase 1 requirements plus:
- Level 2 (C3PAO) in all new solicitations & contracts
- Level 3 (DIBAC) at DoD discretion

CMMC Phase 3

- **Begins 11/10/2027**
- Phase 1 and 2 plus:
- Level 2 (C3PAO) as a condition of award for new contracts and option periods
- Level 3 (DIBCAC) for all applicable solicitations and contracts

CMMC Phase 4

- **Begins 11/10/2028**
- "Full Implementation"
- CMMC requirements included in all applicable DoD solicitations, contracts, and option periods

Varying Agency Perspectives/Standards

- Federal Acquisition Regulatory Council
  - Rule In Progress
  - NIST 800-171r2
  - 8 Hour Reporting Requirements
  - Self Attestation

- General Services Administration
  - GSA Order CIO 2103.2
  - NIST 800-171r3
  - 1 Hour Reporting Requirement
  - RMF Style ATO
- Nuclear Regulatory Commission
  - Management Directive 12.5 / 12.6
  - NIST 800-171r2
  - 8 Hour Reporting Requirement
  - Self Attestation

- Department of Homeland Security
  - HSAR 3052.204-72 (Safeguarding of CUI)
  - DHS Policies / NIST 800-171
  - 1 and 8 Hour Reporting Requirements
  - Self Attestation

- Department of Energy
  - DOE Order 471.7 and C2M2
  - NIST 800-171r2
  - 8 Hour Reporting Requirement
  - Self Attestation
- NASA
  - NASA Procedural Requirement (NPR) 2810.7
  - NIST 800-171r2
  - 1 Hour Reporting Requirement
  - Self Attestation

If a company is Public, pay attention to SEC Reporting Requirements

MSP COLLECTIVE

Cybersecurity & Infrastructure Security Agency (CISA)

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

- Additional Reporting Requirements
  - 24 Hours for Ransomware
  - 72 Hours
    - Substantial Loss of Availability
    - Serious Impact on Safety / Resiliency
    - Unauthorized Access
    - Substantial Confidentiality or Integrity Loss
  - Preserve all relevant data for 2 years
- *Final Rule expected May 2026*

HARMONIZATION is Required!

MSP COLLECTIVE

Exercise: Reporting Nightmare

- You have a MSP / MSSP, your customer SolarTech Solutions is a mid-sized engineering firm that develops specialized cooling systems for high-performance servers. They hold four active contracts:
  - **DoD:** Developing cooling for tactical data centers.
  - **DOE:** Cooling systems for a nuclear research facility.
  - **NASA:** Components for the Artemis moon mission.
  - **GSA:** A standard Schedule contract for commercial server racks.
- **The Incident:** On a Tuesday at 9:00 AM, your security team discovers a **suspected ransomware intrusion**. The attackers have gained "read access" to a file server containing technical drawings and have encrypted several workstations used for project management.

Reporting Deadlines for Suspected Incident

- **NASA**
  - 10AM (1-Hour)
  - Report to NASA SOC
  - Flight related data is Mission Critical
- **DoE**
  - 5 PM (8-Hours)
  - Report to DoE iJC3
  - Involves Nuclear Research Infrastructure
- **GSA**
  - 5 PM (8-Hours)
  - Report to GSA Contracting Officer
  - Report to CISA Incident Portal
  - Suspected CUI Incident
- **CISA / Ransomware**
  - Wednesday 9AM (24 Hours)
  - Report to CISA
  - Ransomware Payment
- **CISA / CIRCIA**
  - Friday 9AM (72 Hours)
  - CIRCIA Report to CISA
- **DoD**
  - Friday 9AM (72 Hours)
  - Report to DIBNet
  - Suspected CUI Incident

MSP COLLECTIVE

ARE YOU PREPARED?

What's an ESP?

Where do MSP's and MSSP's fit in?

MANAGED
SERVICE
PROVIDER
COLLECTIVE

Types of External Service Providers

Cloud Service Provider Definition at USC § 650(3) and 44 USC § 3607: "an entity offering products or services related to cloud computing, as defined by NIST Special Publication 800-145"

800-145 defines five essential characteristics

- On-demand Self Service: Storage, power, etc
- Broad Network Access: Available over the network or internet
- Resource Pooling: Multi-tenency
- Rapid Elasticity: Scale up or down
- Measured Service: You pay for what you use

MSP/MSSP Definition at USC § 650(18):

"an entity delivering services such as network, application, infrastructure or security services via an ongoing and regular support and active administration, on customer premises, in the prodder's data cetner (including hosting), or in a third party data center"

Requirements for CUI

Cloud Service Providers

- FedRAMP Moderate
- FedRAMP Moderate Equivalency
- Not Involved in Assessments
- Documentation Required

Managed (Security) Services Providers

- CUI Processing
  - Must be CMMC L2 / L3 Certified
  - CUI Assets
  - Allows for “Inheritance” …kind of
  - Shared Responsibility Matrix
  - US Persons / US Citizens
- Non-CUI Processing
  - No Certification Requirement
  - Security Protection Assets
  - Must be fully involved in Assessment
  - Shared Responsibility Matrix
  - Beware of Potential Access

MSP COLLECTIVE

What's the Opportunity?

What drove DoD to create this program?

MANAGED SERVICE PROVIDER COLLECTIVE

The Opportunity

- Estimated total size of DIB – 337,968 entities*
- Estimated entities needing CMMC Level 2 (C3PAO) –118,289*
- Estimated entities needing CMMC Level 3 (DIBCAC) – 3,380*
- Letters to supply chain
  - RTX
  - Lockheed Martin
  - Boeing
  - Northrop Grumman
  - Leonardo DRS
  - Leidos
  - Elbit System of America
- The math doesn't math
  - 118,289 L2 x 85% = 100,546 entities
  - 100,546/45 L2 MSPs = 2,234 per L2 MSP
  - 3,380 L3 x 85% = 2,873 entities
  - 2,873/22 L3 MSPs = 124 per L3 MSP

*Department of Defense. (2025). *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)* (90 FR 43573)

MSP COLLECTIVE

Prime Contractor Expectations

LOCKHEED MARTIN

By now, all DIB companies managing CUI should have fully implemented – and be confidently meeting – NIST SP 800-171 (r2) requirements.

Suppliers are encouraged to engage with NIST MEP and/or the CyberAB Marketplace to validate preparedness for an anticipated CMMC third-party assessment and certification.

In addition, by this time all Lockheed Martin suppliers should have transitioned their company self-assessments to the Cybersecurity Compliance and Risk Assessment (CCRA). To assist our programs with understanding and improving their suppliers' CMMC readiness, Lockheed Martin Supply Chain Cybersecurity is reaching out to all suppliers whose latest self-assessment is indicative of unmet cyber requirements (including unimplemented CMMC controls). Ensure you are keeping Lockheed Martin current on your NIST assessment and level of CMMC readiness by

Identify CMMC Gaps to Close

Boeing is readying for the U.S. Department of Defense's (DoD's) final Cybersecurity Maturity Model Certification (CMMC) framework, assessing supplier cybersecurity practices to address gaps.

Reminder for suppliers: Handle Federal Contract Information (FCI) and/or Controlled Unclassified Information (CUI), excluding commercial-off-the-shelf procurements, with the specified CMMC certification to secure contract awards.

For CMMC level 2 certification: Act now. Start preparing for and obtaining certification through a Certified 3rd Party Assessor Organization (C3PAO).

Need assistance? Visit Boeing's Supplier Portal - Cybersecurity Section for resources, including the CMMC Program Preparedness Document and the DoD CMMC website.

Contact Brett Cox, Boeing's CMMC focal, at brett.r.cox@boeing.com / (314) 540-5876.

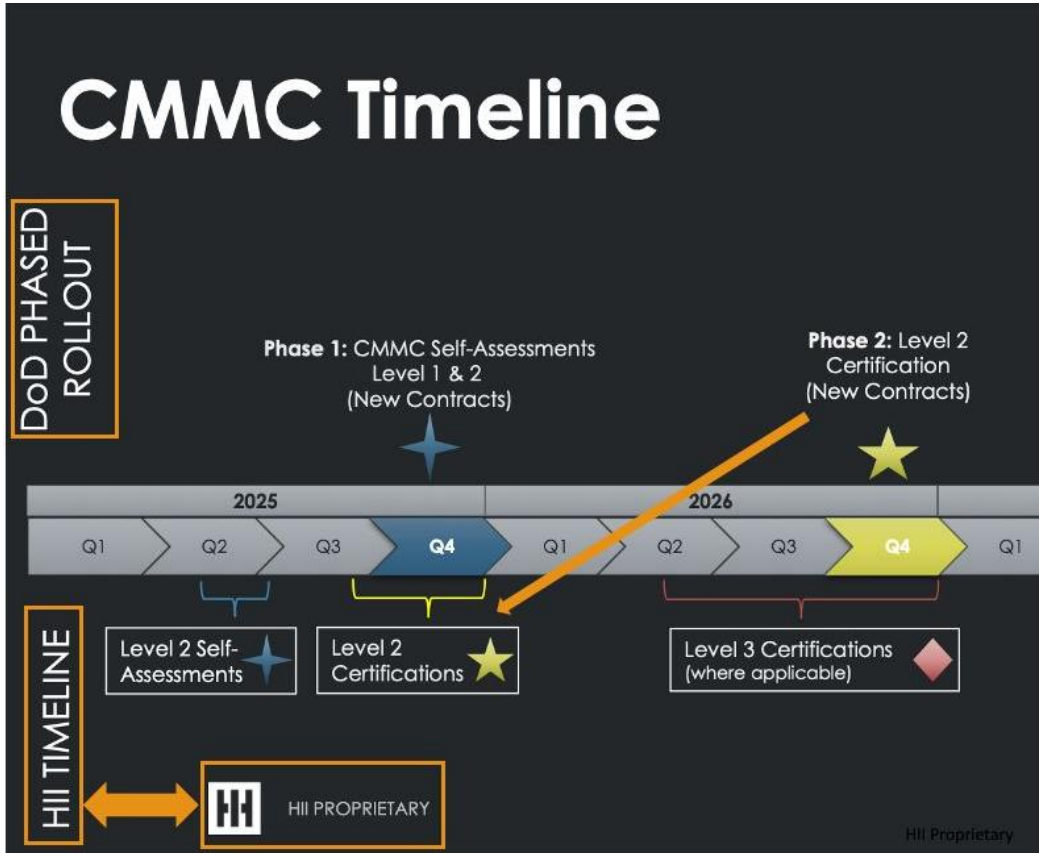
CMMC finalization is expected late this year. Engaging now boosts cybersecurity, keeps future contract eligibility, and ensures sub-tier supplier compliance.

BOEING

Link: https://www.lockheedmartin.com/en-us/suppliers/news/features/2025/cybersecurity-program-rule.html

MSP COLLECTIVE

Prime Contractor Expectations



"This is swimming upstream with our capture team and business development because it is really important that they understand **they just can't pick the best solution or best partner here because I'm getting my best margin return or have a product or capacity to deal with it,"** Williamson said.

Now, they also have to bring forward this sort of **representation of compliance, that's what the government is asking us to do as primes"**

Companies won't be able to do a "six-month sprint" to get prepared because **it could take months, or even a year, to accomplish CMMC compliance.**

-JR Williamson, CISO

MSP COLLECTIVE

Participation in Customer Assessments

With and Without the CMMC Level 2 Cert

MANAGED SERVICE PROVIDER COLLECTIVE

Participation in Customer Assessments: With and Without Your Own CMMC L2 Certification

Real life experience of what an assessment is like:

- Specific & Detail Oriented
- Significant Preparation
- Addressing EACH of the Assessment Objectives
- Understanding the FULL Assessment Scope, Including the MSP Network
- MSP L2 Cert – MSP Network Doesn't Need to be Assessed, Services Still Do
- C3PAO Take on Whether the MSP is Already Level 2 Certified

MSP COLLECTIVE

Leveraging a GRC platform

Single source of truth for compliance tracking:

- Determination Statements
- Policies
- Incident Response Plan
- Inventory Management
- Artifact/ Evidence Storage
- POA&Ms
- Operations Plans of Action
- Risk Assessments

MSP COLLECTIVE

Data Types

CMMC is all about CONFIDENTIALITY of Data

MANAGED
SERVICE
PROVIDER
COLLECTIVE

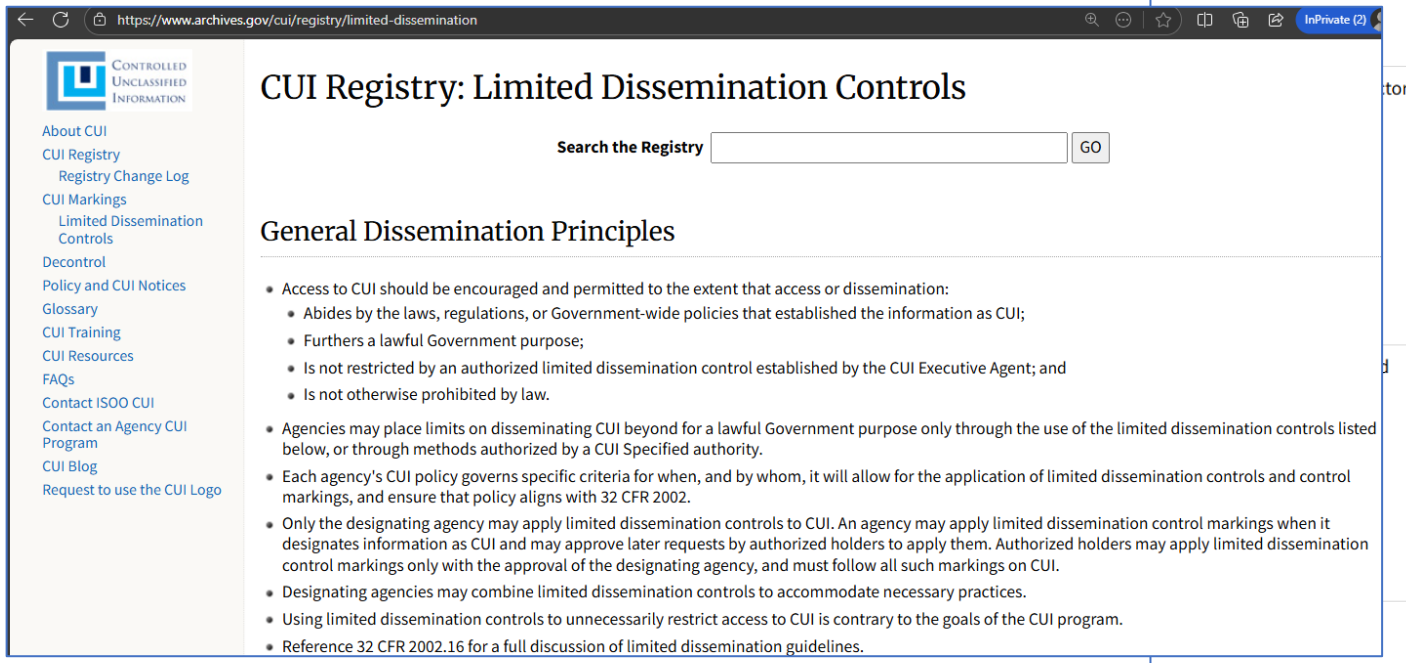
Types of Data

FCI – Federal Contract Information (Level 1)
"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 (Level 2)
"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-side policy requires or permits an agency to handle using safeguarding or dissemination controls."

Basic vs. Specified CUI
Why it's important

A Word About Dissemination Controls



Limited Dissemination Control	Description	Marking	Portion Marking
No foreign dissemination	Information may not be disseminated in any form to foreign governments, foreign nationals, foreign or international organizations, or non-US citizens.	NOFORN	NF
Federal employees only	Dissemination authorized only to (1) employees of United States Government executive branch departments and agencies (as the agency is defined in 5 U.S.C. 105), or (2) armed forces personnel of the United States or Active Guard and Reserve (as defined in 10 USC 101).	FED ONLY	FED ONLY
Federal employees and contractors only	Dissemination authorized only to (1) employees of United States Government executive branch departments and agencies (as the agency is defined in 5 U.S.C. 105), (2) armed forces personnel of the United States or Active Guard and Reserve (as defined in 10 USC 101), or (3) individuals or employers who enter into a contract with the United States (any department or agency) to perform a specific job, supply labor and materials, or for the sale of products and services, so long as dissemination is in furtherance of that contractual purpose.	FEDCON	FEDCON
tors	No dissemination authorized to individuals or employers who enter into a contract with the United States (any department or agency) to perform a specific job, supply labor and materials, or for the sale of products and services. Note: This dissemination control is intended for use when dissemination is not permitted to Federal contractors, but permits dissemination to state, local, or tribal employees.	NOCON	NOCON
d	Dissemination authorized only to those individuals, organizations, or entities included on an accompanying dissemination list. Note: Use of this limited dissemination control supersedes other limited dissemination controls, but cannot supersede dissemination stipulated in law, Federal regulation, or Government-wide policy.	DL ONLY	DL ONLY
	A permissive foreign disclosure and release marking used on information to indicate that the originator has authorized a Senior Foreign Disclosure and Release Authority (SFDRA) to make further sharing decisions for uncaveated intelligence material (intelligence with no restrictive dissemination controls) in accordance with existing procedures, guidelines, and	RELIDO	RELIDO

MSP COLLECTIVE

Types of Data

SPD – Security Protection Data (Level 2)

Security Protection Assets provide security functions or capabilities within the OSA's CMMC Assessment Scope.

Security Protection Assets are part of the CMMC Assessment Scope and are assessed against Level 2 security requirements that are relevant to the capabilities provided. For example, an External Service Provider (ESP), defined in 32 CFR §170.4, that provides a security information and event management (SIEM) service may be separated logically and may not process CUI, but the SIEM does contribute to meeting the CMMC requirements within the OSA's CMMC Assessment Scope. Table 2 provides examples of Security Protection Assets.

Security Protection Data means data stored or processed by Security Protection Assets that are used to protect an OSA's assessed environment.

Security Protection Data is security-relevant information which, if disclosed, could aid an attacker in the compromise of the system. It includes, but is not limited to:

- ***configuration data required to operate a security protection asset,***
- ***log files generated by or ingested by a security protection asset,***
- ***data related to the configuration or vulnerability status of in-scope assets, and***
- ***passwords that grant access to the in-scope environment.***

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP COLLECTIVE

Asset Type

Data	Asset Type	Requirement	Entity	Certification
CUI	CUI Asset	800-171	Internal	OSA
CUI	Cloud CUI Asset	FedRAMP	Internal	OSA
SPD	ESP Asset	800-171	Internal	OSA
SPD	ESP Asset	800-171	External (MSP)	MSP
-	SPA	800-171	Internal	OSA
-	SPA	800-171	External (MSP)	MSP

Courtesy: Ryan Bonner, Daniel Akridge CS2 2024

Scoping

As an MSP, what all comes into scope?

MSP
MANAGED
SERVICE
PROVIDER
COLLECTIVE

Scoping

1. Identify the facilities, equipment, software, people, tools (mechanisms) and data flow that will be leveraged in support of your DIB customers.

2. Categorize by type of Asset. Most will be CUI or SPA. Clearly identify Out of Scope assets – just as important as in-scope categories.

3. Prepare to defend your boundary.
    - Understand where your external connections are and how they are controlled.
    - Understand internal physical and logical boundaries, not just external.

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP COLLECTIVE

Asset Categories

Where most MSP's & MSSP's are going to land

Pay attention to "Requirements"

Category	Asset Description	OSA Requirements	CMMC Assessment Requirements
Assets that are in the Level 2 CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	o Assets that process, store, or transmit CUI	o Document in the asset inventory o Document asset treatment in the System Security Plan (SSP) o Document in the network diagram of the CMMC Assessment Scope o Prepare to be assessed against CMMC Level 2 security requirements	o Assess against all Level 2 security requirements
Security Protection Assets	o Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope	o Document in the asset inventory o Document asset treatment in SSP o Document in the network diagram of the CMMC Assessment Scope o Prepare to be assessed against CMMC Level 2 security requirements	o Assess against Level 2 security requirements that are relevant to the capabilities provided
Contractor Risk Managed Assets	o Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place	o Assets are not required to be physically or logically separated from CUI assets o Document in the asset inventory o Document asset treatment in the SSP o Document in the network diagram of the CMMC Assessment Scope o Prepare to be assessed against CMMC Level 2 security requirements	o Review the SSP: i. If sufficiently documented, do not assess against other CMMC securityrequirements, except as noted ii. If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies iii. The limited check(s) shall not materially increase the assessment duration nor the assessment cost iv. The limited check(s) will be assessed against CMMC security requirements
Specialized Assets	o Assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment	o Document in the asset inventory o Document asset treatment in the SSP o Show these assets are managed using the contractor's risk-based security policies, procedures and practices o Document in the network diagram of the CMMC Assessment Scope	o Review the SSP o Do not assess against other CMMC security requirements
Assets that are not in the Level 2 CMMC Assessment Scope			
Out-of-Scope Assets	o Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets	o Assets that are physically orlogically separated from CUI assets o Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset o An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset o Prepare to justify the inability of an Out-of-Scope Asset to store, process, or transmit CUI	o None

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP COLLECTIVE

SPA's

Table 2. Security Protection Asset Examples

Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who implement system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facilities	• Co-located data centers • Security Operations Centers (SOCs) • OSA office buildings

If your MSP/MSSP outsources services that involve humans or tools accessing the endpoints or servers of your customers, they would be in scope and require their own CMMC L2 self-assessment (or Certification) with a Shared Responsibility Matrix.

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP Roles & Responsibilities – All Practices

Basic
Intermediate
Advanced

CMMC Level 1

AC	IA	MP	PE	SC	SI
AC.L1-3.1.1	IA.L1-3.5.1	MP.L1-3.8.3	PE.L1-3.10.1	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.2	IA.L1-3.5.2		PE.L1-3.10.3	SC.L1-3.13.1	SI.L1-3.14.4
AC.L1-3.1.20			PE.L1-3.10.4		SI.L1-3.14.5
AC.L1-3.1.22			PE.L1-3.10.5		SI.L1-3.14.1

CMMC Level 2

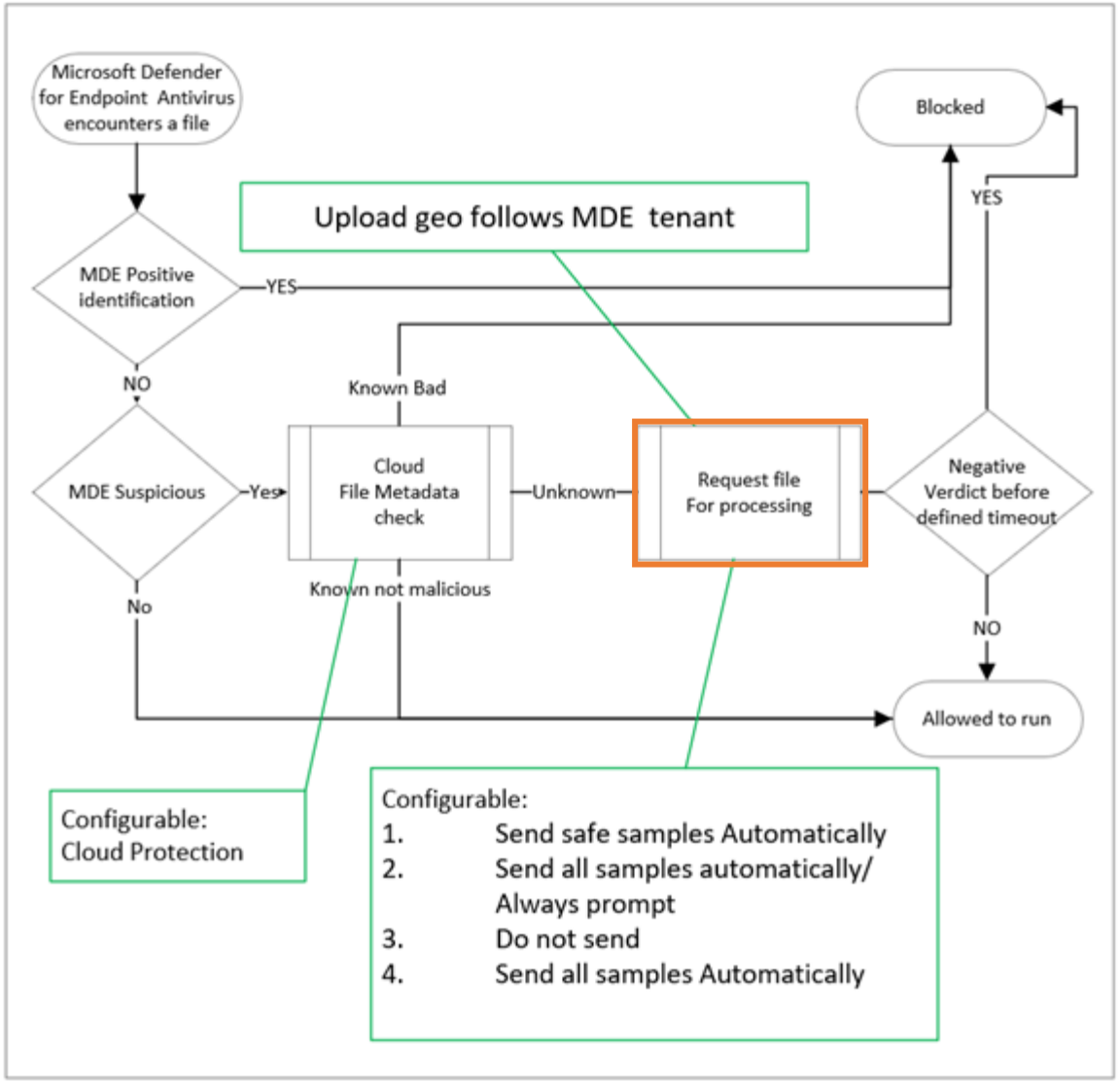
AC	AT	AU	CA	CM	IA	IR	MA	MP	PE	PS	RA	SC	SI
AC.L1-3.1.1	AT.L2-3.2.1	AU.L2-3.3.1	CA.L2-3.12.1	CM.L2-3.4.8	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L2-3.8.7	PE.L2-3.10.2	PS.L2-3.9.1	RA.L2-3.11.1	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.2	AT.L2-3.2.2	AU.L2-3.3.2	CA.L2-3.12.2	CM.L2-3.4.9	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L1-3.8.3	PE.L1-3.10.1	PS.L2-3.9.2	RA.L2-3.11.2	SC.L1-3.13.1	SI.L1-3.14.4
AC.L1-3.1.20	AT.L2-3.2.3	AU.L2-3.3.4	CA.L2-3.12.3	CM.L2-3.4.1	IA.L2-3.5.11	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.1	PE.L1-3.10.3		RA.L2-3.11.3	SC.L2-3.13.14	SI.L1-3.14.5
AC.L2-3.1.12		AU.L2-3.3.7	CA.L2-3.12.4	CM.L2-3.4.2	IA.L2-3.5.7		MA.L2-3.7.4	MP.L2-3.8.2	PE.L1-3.10.4			SC.L2-3.13.15	SI.L2-3.14.3
AC.L2-3.1.16		AU.L2-3.3.8		CM.L2-3.4.3	IA.L2-3.5.9		MA.L2-3.7.5	MP.L2-3.8.4	PE.L1-3.10.5			SC.L2-3.13.2	SI.L1-3.14.1
AC.L2-3.1.17		AU.L2-3.3.9		CM.L2-3.4.4	IA.L2-3.5.10		MA.L2-3.7.6	MP.L2-3.8.5	PE.L2-3.10.6			SC.L2-3.13.3	SI.L2-3.14.6
AC.L1-3.1.22		AU.L2-3.3.3		CM.L2-3.4.5	IA.L2-3.5.3			MP.L2-3.8.6				SC.L2-3.13.4	SI.L2-3.14.7
AC.L2-3.1.4		AU.L2-3.3.5		CM.L2-3.4.6	IA.L2-3.5.4			MP.L2-3.8.8				SC.L2-3.13.6	
AC.L2-3.1.5		AU.L2-3.		CM.L2-3.4.7	IA.L2-3.5.5			MP.L2-3.8.9				SC.L2-3.13.7	
AC.L2-3.1.6					IA.L2-3.5.6							SC.L2-3.13.8	
AC.L2-3.1.8					IA.L2-3.5.8							SC.L2-3.13.9	
AC.L2-3.1.10												SC.L2-3.13.10	
AC.L2-3.1.11												SC.L2-3.13.11	
AC.L2-3.1.13												SC.L2-3.13.12	
AC.L2-3.1.14												SC.L2-3.13.13	
AC.L2-3.1.21												SC.L2-3.13.16	
AC.L2-3.1.3													
AC.L2-3.1.7													
AC.L2-3.1.9													
AC.L2-3.1.15													
AC.L2-3.1.18													
AC.L2-3.1.19													

MSP COLLECTIVE

Credit: Edwards Performance Solutions

EDR

Most EDR tools automatically upload files to the cloud for detonation and analysis.

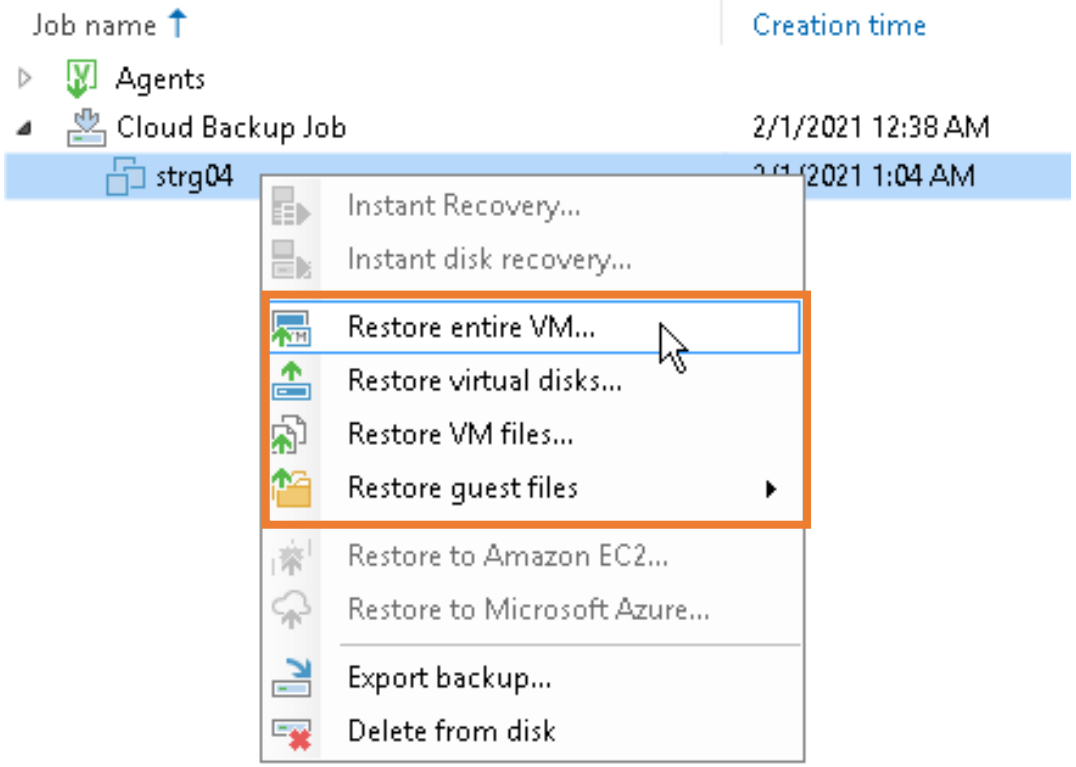


Courtesy: Ryan Bonner, Daniel Akridge CS2 2024

MSP COLLECTIVE

Data Backups

Many data backup services have the keys to decrypt and restore backup images or files.

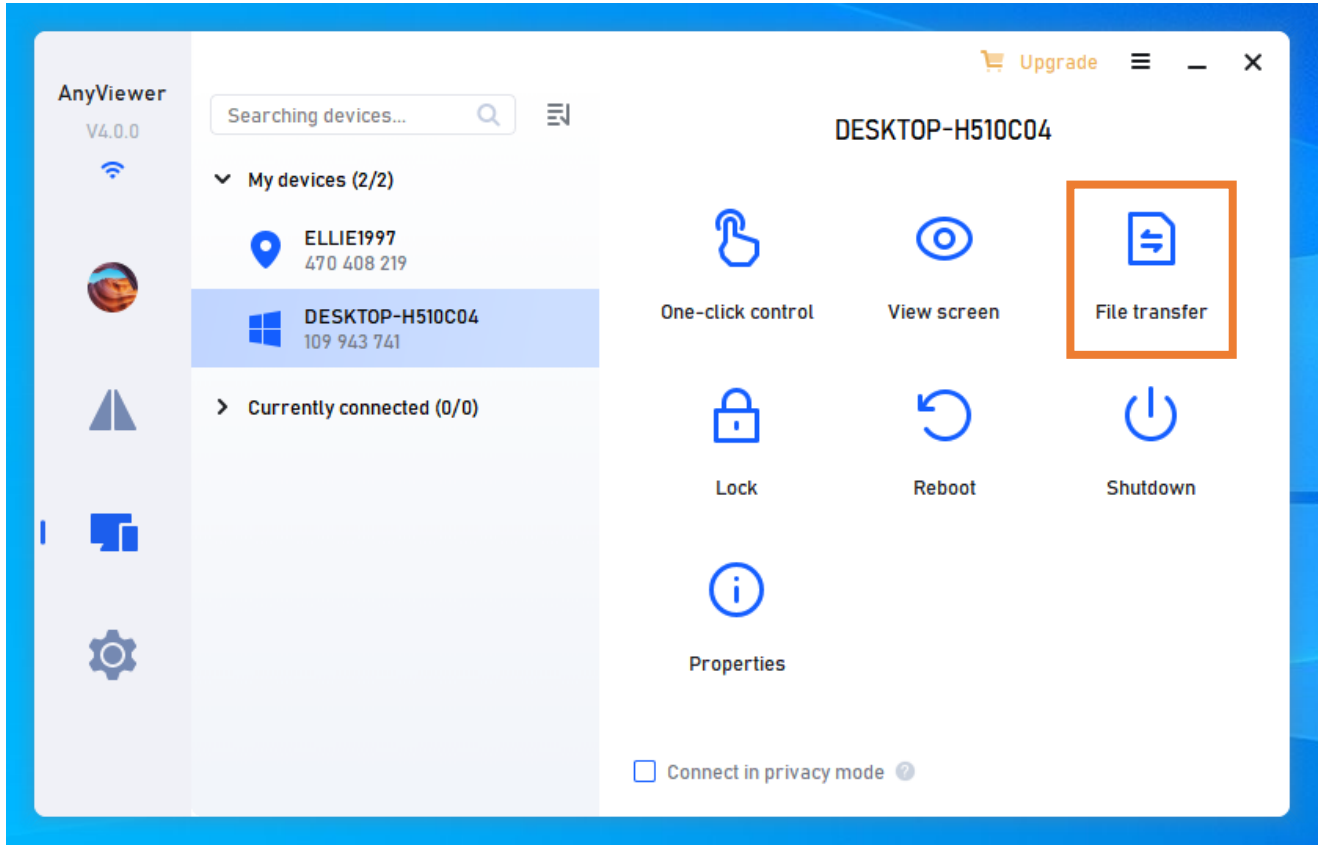


Courtesy: Ryan Bonner, Daniel Akridge CS2 2024

MSP COLLECTIVE

RMM

Many RMM tools allow personnel to transfer files to helpdesk technicians.



Courtesy: Ryan Bonner, Daniel Akridge CS2 2024

Where Does the Data Flow? Who Touches It?

MFA
AAD/ADFS
Intune
Conditional Access
Ports
Azure Firewall
Information Protection
E-Mail Communications
Repositories

Backups
MXDR
SIEM
Log Analytics
Printing
WiFi Access
Badging System
Camera System

Sales
Contracts
Engineers, Architects
Helpdesk
SOC
HR
Facility Maintenance
Executives
Outsourced Support

MSP COLLECTIVE

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

Defend Your Scope

SPA Components (ESP)

SP Assets

Roles

Per RBAM

MSP & MSSP Roles

Facilities

S7 Headquarters – Huntsville, AL
MS USGov Datacenter (inherited)
ITSM Solution USGov Datacenter (inherited)
Backup Solution USGov Datacenter (inherited)

Technologies & Equipment

Cloud

MS 365 GCC-H (FedRAMP)
Azure Gov (FedRAMP)
ITSM Solution USGov (FedRAMP)
Backup Solution USGov (FedRAMP)
MFA Solution (FedRAMP)
Password Mgmt Solution (FedRAMP)

On-Prem

Managed Desktops, Laptop, Servers
iOS, Android Mobile Devices
Printers? USB Drives? Scanners? Syslog Server, Vulnerability Scanner, Linux Server, Firewall, APs, Switches, Badging, CCTV ….

CRMA Assets

DocuSign? Home Printers?

Out of Scope Assets ISP? Home Offices? Guest Wireless? AVDs with only keyboard/mouse/video pass through?

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP COLLECTIVE

Defend Your Scope

CUI Components (DIB)

CUI Assets

Roles
Per RBAM

Facilities

Technologies & Equipment

Cloud

On-Prem

CRMA Assets

Out of Scope Assets ISP? Home Offices? Guest Wireless? AVDs with only keyboard/mouse/video pass through?

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP COLLECTIVE

Understand What Level 3 Means for Scoping and Asset Categorization

Because the scoping of a Level 2 assessment is not the same as the scoping of a Level 3 assessment, before determining the CMMC Assessment Scope it is important to first consider if the organization will seek a CMMC Status of Final Level 3 (DIBCAC). **If the intent is to obtain a CMMC Status of Final Level 3 (DIBCAC), the OSC should also consider the guidance provided in the CMMC Scoping Guide – Level 3 document.**

Assets designated as Contractor Risk Managed Assets (CRMAs) in the Level 2 CMMC Assessment Scope are treated as CUI assets if they fall within the Level 3 CMMC Assessment Scope. OSCs may choose to designate them as CUI Assets for the Level 2 certification assessment and have them assessed by a C3PAO.

Since the assessment requirements for Specialized Assets differ between Level 2 and Level 3, the OSC may choose to have them assessed by a C3PAO during the Level 2 certification assessment. **During a Level 3 certification assessment, DCMA DIBCAC may check any Level 2 security requirement of any in-scope asset.**

CRMAs and Specialized Assets not assessed to the Level 3 scoping requirements by a C3PAO during the Level 2 certification assessment will undergo limited checks for compliance with Level 2 security requirements during the DCMA DIBCAC certification assessment.

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP COLLECTIVE

Implementation

What's Your Best Approach?

MANAGED
SERVICE
PROVIDER
COLLECTIVE

Implementation Considerations

Infrastructure

- Either Fully Uplift entire support infrastructure or build a second infrastructure
- Ensure all Infrastructure involved in Customer Delivery is “In Scope”
- Ensure the SRM accurately defines who, what, when and how for all 320 Assessment Objectives
- Timeline for a MSP / MSSP is 18-24 Months for Level 2

Budget

- The DIB and MSPs are considered “Regulated Industries”
- Investment in time, hardware and software is easily 1M+ over 2 years
- Expect 8-10% of Revenue to run Internal IT and Compliance for a Regulated MSP/MSSP for Level 2

MSP COLLECTIVE

Critical Documents

- Data Flow Diagram
- Infrastructure Diagram
- Boundary Diagram
- Inventory of All Assets
- Policies & Procedures to Cover Every Domain
- Risk Register
- Change Control Board
- SRM – Yours, and the CSPs, and Other Outsourced Capabilities
- SSP
- POA&M (Gap Assessment Results & Remediation of All Items

Source: CMMC Scoping Guide Level 2, Version 2.13 | Sept 2024

MSP COLLECTIVE

The Shared Responsibility Matrix

I keep hearing about this darn "SRM"

MANAGED SERVICE PROVIDER COLLECTIVE

Shared Responsibility Matrix - MSP

No Responsibility | Shared Responsibility | Full Responsibility

Category Name	CMMC 2.0	NIST Control Statement	AO	Assessment Objectives	MSP Procedure and/or Evidence	MSP Information Provided to Client for Authorization	MSP Services – Azure Package
Access Control (AC)	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	3.1.3[a]	[a] information flow control policies are defined.			
			3.1.3[b]	[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.		x	Informational: MSP will consult with the customer on the enforcement mechanisms available within the customer's work package and …
			3.1.3[c]	[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]	[d] authorizations for controlling the flow of CUI are defined.		x	Informational: MSP will consult with the customer on the enforcement mechanisms available within the customer's work package and …
			3.1.3[e]	[e] approved authorizations for controlling the flow of CUI are enforced.	x		Implementation Summary: MSP enforces information flow control through AD/AAD, AIP (MIP)/UL, and …

MSP COLLECTIVE

Shared Responsibility Matrix – Microsoft 365

No Responsibility | Shared Responsibility | Full Responsibility

Category Name	CMMC 2.0	NIST Control Statement	AO	Assessment Objectives	MS Procedure and/or Evidence	Microsoft Azure SSP (AC - 03)
Access Control (AC)	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	3.1.3[a]	[a] information flow control policies are defined.		Be sure to check the mapping from NIST 800-53A R5 (FedRAMP) to NIST 800-171A R2. Why?
			3.1.3[b]	[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.		
			3.1.3[c]	[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]	[d] authorizations for controlling the flow of CUI are defined.		
			3.1.3[e]	[e] approved authorizations for controlling the flow of CUI are enforced.	x	

MSP COLLECTIVE

AC-04(04) Flow Control of Encrypted Information Microsoft 365

AC-04(04) Control Summary Information
Responsible Role: Customer Administrator, Service Engineer Operations
Parameter AC-04(04)-1: intrusion detection mechanisms
Parameter AC-04(04)-2: blocking the flow of encrypted information
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing authorization

AC-04(04) What is the solution and how is it implemented?

Customer Responsibility

Government customers are responsible for preventing encrypted information from bypassing content-checking mechanisms by (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; organization-defined procedures or methods. M365 supports customer compliance with M-21-31 and M-22-09.

M365

M365 prevents encrypted information from bypassing IDS through implementing information flow control by allowing only connections and communication which are necessary to allow systems to operate, blocking all other ports, protocols and connections by default. This includes intra-service communications as well as connections to external information systems. Access Control Lists (ACLs) are the preferred mechanism to restrict network communications by source and destination networks, protocols, and port numbers. ACLs exist at both the host and network level. M365 manages ACL approvals through the Request For Change (RFC) process (including review and risk acceptance) and the change process, and Azure implements the approved change. Approved mechanisms to implement networked-based ACLs include: ACLs on routers managed by Azure and firewall rules.

The use of firewall rules and ACLs allows M365 to control the flow of information within the system and between interconnected systems. The use of the RFC process ensures that data flows are authorized and approved.

Service teams also employ HostIDS to further monitor for data exfiltration at the host level. NRT is used to alert based on specific security events as well as other indicators of compromise, through Vanquish, such as anomalous behavior and suspicious activity.

Shared Responsibility Matrix - Customer

No Responsibility | Shared Responsibility | Full Responsibility

Category Name	CMMC 2.0	NIST Control Statement	AO	Assessment Objectives	Cust Procedure and/or Evidence	S7 Information Provided to Client for Authorization	Customer
Access Control (AC)	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	3.1.3[a]	[a] information flow control policies are defined.	x		Customer defines information flow control policies
			3.1.3[b]	[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.		x	Informational: Summit 7 will consult with the customer on the enforcement mechanisms available within the customer's work package and support services for information flow control. Mechanisms are established via work package build and are managed within the bounds of the managed service agreements.
			3.1.3[c]	[c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.	x		Customer defines designated sources and destinations for CUI
			3.1.3[d]	[d] authorizations for controlling the flow of CUI are defined.		x	Informational: Summit 7 will consult with the customer on the enforcement mechanisms available within the customer's work package and support services for information flow control. Mechanisms are established via work package build and are managed within the bounds of the managed service agreements.
			3.1.3[e]	[e] approved authorizations for controlling the flow of CUI are enforced.			MSP Responsibility

MSP COLLECTIVE

Shared Responsibility Matrix – Combined Picture

No Responsibility | Shared Responsibility | Full Responsibility

Category Name	CMMC 2.0	NIST Control Statement	AO	Assessment Objectives	MSP	Microsoft	Customer
Access Control (AC)	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	3.1.3[a]	[a] information flow control policies are defined.			
			3.1.3[b]	[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.			
			3.1.3[c]	[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]	[d] authorizations for controlling the flow of CUI are defined.			
			3.1.3[e]	[e] approved authorizations for controlling the flow of CUI are enforced.			

MSP COLLECTIVE

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.

The System Security Plan

The Only Control That Fails the Whole Assessment if Done Wrong (or missing)

MANAGED SERVICE PROVIDER COLLECTIVE

The SSP

- Backbone of the assessment
- Write at the assessment objective level
- Represent all asset categories
- Ensure alignment with supplementary documentation
  - Policy
  - Procedure
  - System Configuration
  - Incident Response Plan
- Say what you do and do what you say
- Be thorough but concise

MSP COLLECTIVE

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

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

Control Status: [Fully Implemented and Full Inheritance, Fully Implemented and Partial Inheritance, Implemented and No Inheritance, Planned, or Not Applicable]	
Inherited From:	
[a]	All authorized users are identified via the Company's Authorized Users list. All Company employees, external guests, and/or users accessing Company CUI in systems and networks are added to the list when such access is authorized by the

	CMMC Lead or Company Official. Account creation requests are submitted to the Managed Services Security Provider (MSSP) ticketing system, HaloPSA. The Authorized Users list is maintained by the Company and the Company's MSSP. Company MSSP is notified via HaloPSA when a Company employee, external guest, or external user no longer requires access to the Company's CUI systems and network, and the user is removed from the directory services and the Authorized Users List.
[b]	Service accounts for executing processes on behalf of the authorized users are identified in the Authorized Users list. The processes those services accounts are performing are identified in Entra ID and the Information Management Program Manual (IMPM) under Access Control.

	Authorized Users List.
[b]	Service accounts for executing processes on behalf of the authorized users are identified in the Authorized Users list. The processes those services accounts are performing are identified in Entra ID and the Information Management Program Manual (IMPM) under Access Control. Non-interactive sign-in logs in Entra ID identify sign-ins that were performed by a Company app or an OS component on behalf of the user (e.g., Single Sign On (SSO) is utilized for authentication). All scripts pushed from Intune to authorized endpoints are run in the system context, not the user context. All scripts are manually created and configured by Company's MSSP.
[c]	All devices authorized to connect to the system are identified in Company Hardware Accountability Inventory, Microsoft Intune, and Entra ID.
[d]	System access is limited to authorized Company employees, external guests, and external users authorized by the CMMC Lead [If there are any other roles within the company with permission to authorize access list those here] via Entra ID authentication. The Company enforces various Entra ID conditional access policies to ensure system access is limited to only authorized users. Company reviews active user rosters in Entra ID and compares it to the current Company Authorized Users list.
[e]	System access to processes acting on behalf of authorized users are enforced by Entra ID and RBAC roles.
[f]	Company uses Entra ID conditional access policies to limit system access to authorized devices. Devices belonging to authorized Company users who do not satisfy these conditional access policies in Entra ID are prevented access to Company authorized resources. [If GFE is used and there is no network segmentation to take GFE out of scope, include the following, otherwise remove: Authorized users who primarily work on GFE are not subject to these policies because they are permitted access to CUI on the Company network or on Company systems.]

	[If GFE is used and those GFE users are permitted mobile access to CUI outside of their GFE, but are not permitted a designated Company managed device, include

Resources

You're not alone!

MANAGED SERVICE PROVIDER COLLECTIVE

Resources

1. Official Governance Source Docs & Resources
   - https://www.archives.gov/cui/registry/category-list
   - https://dodcio.defense.gov/CMMC/Resources-Documentation/ - read the CAP!
   - https://dowcio.war.gov/Portals/0/Documents/CMMC/CMMC-FAQsv4.pdf
   - CyberAB > Directory

2. Certification (CCP, CCA) Highly Recommended
   - CMMC-AB Certification Training | Edwards Performance Solutions
   - Available CMMC Courses | WTI Networks
   - Training | Space Coast Cyber

3. Conferences, Podcasts, and more
   - Home - CS5 West | The Official Conference of The Cyber AB
   - CMMC Day 2026 Registration – DIB Cyber Certification Series
   - Home - CS5 East 2025 - The Essential Event to Get CMMC Right
   - Summit 7 – YouTube
   - Climbing Mount CMMC The Podcast - Axiom

Q&A

MSP COLLECTIVE

How Can We Help?

Learn More

info@mspcollective.org

mspcollective.org

MSP

MANAGED
SERVICE
PROVIDER
COLLECTIVE