

TALES FROM THE TRENCHES

Why OSCs Fail Their
CMMC Level 2 Certification



Speakers



Tobias Musser

Co-CEO
MNS Group



Fernando Machado

Managing Principal/CISO
Cybersec Investments



A CMMC Level 2 Certified MSP/MSSP

STAFFED BY:

CMMC Certified Professionals (73 CCP)

CMMC Certified Assessors (40+ CCA's)

Registered Practitioners (100% Staff RP's)

OVERVIEW

- Headquarters in Maryland – Supporting 300+ locations worldwide
- Security and compliance-focused
- Modeled on a risk framework, we assist our partners to identify and minimize risk areas: operational, financial, technological, human, vendor, client, and reputational.
- Committed to protecting the USA, business by business.

SecureCMMCSM



SecureCMMCSM Enclave Trusted by 20% of C3PAO's

Professionals use MNS Group's FedRAMP High Assessment Enclave System, with all STIG's applied.

www.securecmmc.com



Fernando Machado

CISO, Cybersec Investments

- **Cybersecurity Experience:**

- 15+ years DoD cybersecurity experience
- NIST 800-171: Controlled Unclassified Information (CUI) / Cybersecurity Maturity Model Certification (CMMC)
- Army, Navy, Air Force customer experience

- **Certified:**

- Lead CMMC Certified Assessor (Lead CCA)
- Certified CMMC Professional (CCP)
- Authorized CMMC 3rd Party Assessment Organization (C3PAO)

- **Awards:**

- President's Volunteer Service Award



1900 S Harbor City Blvd. Suite 340
Melbourne, Florida 32901

info@cybersecinvestments.com

1-800-960-8802

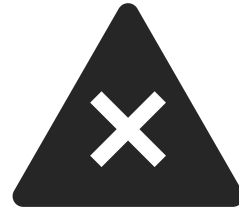


The Urgency of CMMC Certification



CMMC is no longer theoretical.

It's active and required for defense contracts.



CMMC Gatekeeping

Certification (Self or C3PAO) determines contract eligibility and competitiveness.



C3PAOs are booking out months in advance.

Delays mean lost opportunities for contractors.

What C3PAOs Are Seeing



Waitlisting

A growing backlog of companies seeking assessments



Underestimating the Workload

Many OSCs are underestimating the time and steps to prepare for their assessment



Larger Scope Than Expected

The assessment is more rigorous and detailed than many expect

01

The CMMC Bottleneck



Why OSCs are struggling to implement CMMC.

- Lack of internal resources or expertise.
- Waiting too long to start documentation and remediation.
- Misconceptions about the assessment process (it's NOT a simple checklist).
- CMMC-Literate professionals are booking out.



02

Common Compliance Pitfalls



Critical, but avoidable issues during the assessment

- Incomplete or inaccurate System Security Plan (SSP)
- Failure to properly identify CUI
- Security measures not fully implemented
- Supply chain issues, relying on non-compliant subcontractors, ESPs, and CSPs



03

SSP (System Security Plan) Shortfalls



Certification Killer: Insufficient SSP

- Common Mistakes: generic, copy-paste, “We do” statements or outdated SSPs.
- Assessors expect detailed, accurate, and organization-specific documentation
- Not ensuring your SSP is assessment-ready



04

Improper CUI Identification



Not protecting or identifying the right assets

- Confusion over what **is** and **is not** CUI.
- The importance of Security Protection Assets (SPA).
- Ensuring Customer Relationship Management (CRM) systems comply.



05

Insufficient Muscle Memory



Practice on-paper not aligning with real-time discipline

- Weak operational proof of implementation
- POA&M discipline missing
- “Show me, don’t tell me.” Assessors look for evidence of implementation

A Successful Assessment



Documentation

Well-documented security controls, policies, and procedures.



Organization

Artifacts are organized in the package, and it is easy for assessors to identify them at the objective level.



Teamwork

A confident, prepared team that understands their security roles.



Preparation

No last-minute remediation—controls must be in place for assessment.

Fixing Common Documentation Gaps

**Missing or
vague policies**



Develop the evidence of
implementation Assessors require

**Insufficient
Planning**



Build effective Plans of
Action & Milestones

**Lack of
Evidence**



Provide evidence for (MFA) Multi-
factor authentication, encryption,
and incident response

Choosing the Right Path

DIY, Consultants, or Full MSP Support?

- Internal team vs. external consultants:
Weighing cost vs. expertise.
- The role of C3PAOs, RPOs, and MSPs in helping you prepare.
- Avoiding scams and misinformation—how to vet your support team.

Benefits of Getting Assessed NOW

- ✓ Leaders will have a first-mover advantage
- ✓ Ability to bid on CMMC “gated” contracts
- ✓ Have 36 months to get ready for Rev 3
 - Attract and maintain top talent who want to
- ✓ be among best
- ✓ Business continuity
 - Attractive to investors



WARNING:

The Cost of Waiting:
emergency remediation is far more expensive than proactive planning, CMMC Assessment is more expensive when scheduled within 1-2 months of need.

Final Checklist

Are You Truly Ready for Your CMMC Assessment?

- ✓ How ready you are determines how compliant you will STAY
- ✓ Practices implemented IRL minimize the risk of the False Claims Act.
- ✓ A last look at readiness: Documentation, staff readiness, artifact organizations
- ✓ Where to go for expert guidance and resources



THANK YOU

MNS Group

 ask@mnsgroup.com

 www.mnsgroup.com/ask

Cybersec Investments

 info@cybersecinvestments

 <https://cybersecinvestments.com>