Cyber & Cybersecurity Maturity Model Certification (CMMC)

April 30, 2026

The Panelists

Donnie Hill

CISO | Cyber Risk & Resilience
Kiewit

402.342.2052

Donnie.hill@kiewit.com

Reggie Jones

Partner | Chair of Federal Government Contracts
Fox Rothschild LLP

202.461.3111

rjones@foxrothschild.com

David Tomlinson

General Counsel
Massman Construction

913.291.2600

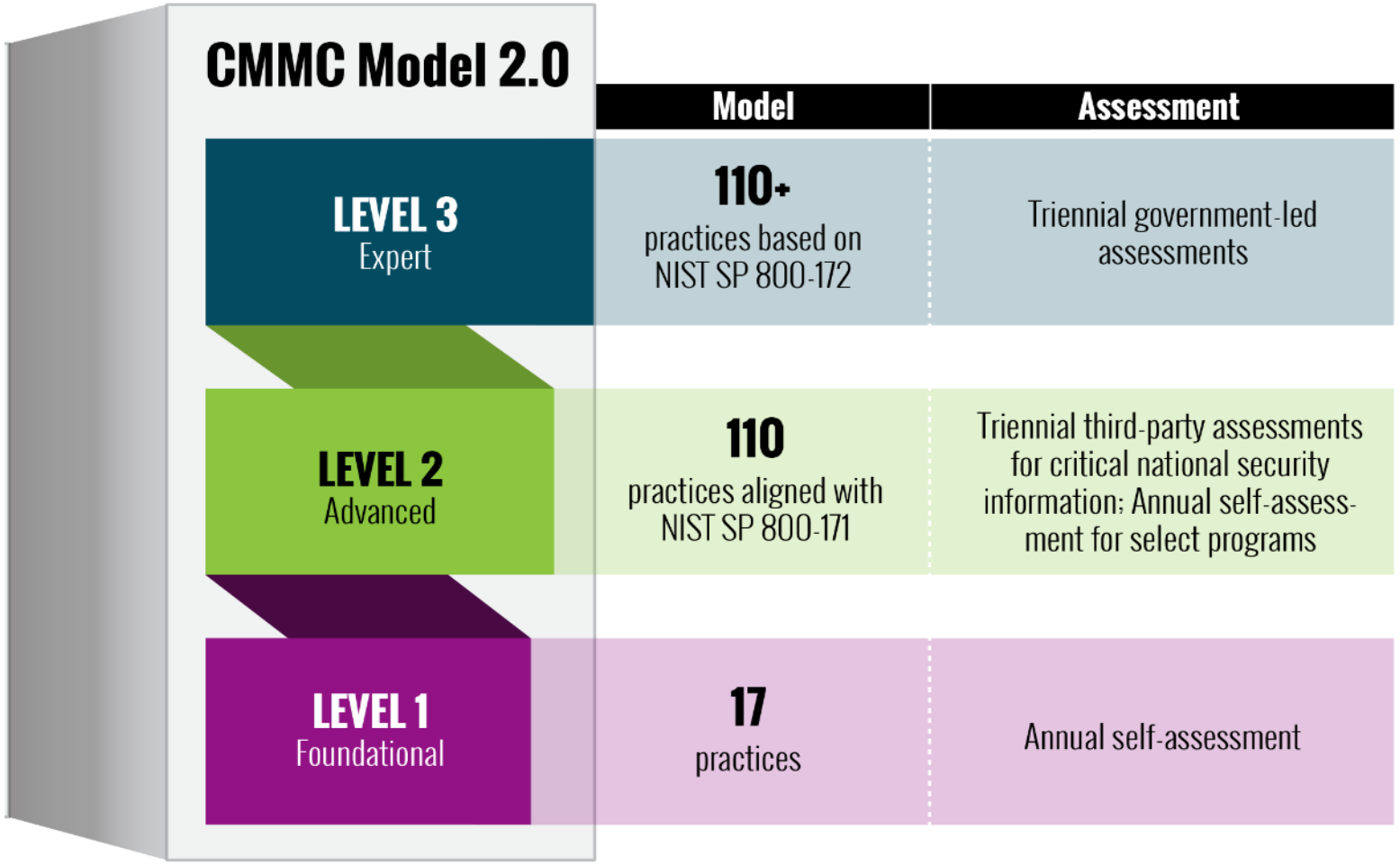
dtomlinson@massman.net

What is the Cybersecurity Maturity Model Certification (CMMC)?

- A mandatory certification of DOD contractors' and subcontractors' information systems that is intended to protect not only sensitive but also unclassified data against cyber threats.
- Created with federal funding by Carnegie Mellon University & Johns Hopkins University Applied Physics Laboratory, LLC
- CMMC 1.0 released on January 30, 2020; DOD announced CMMC 2.0 on November 17, 2021
- DOD issued final rule implementing the CMMC program at **32 CFR Part 170** and in the DFARS at 48 CFR Parts 204, 212, 217, and 252
  - Cybersecurity Maturity Model Certification (CMMC) Program (89 Fed. Reg. 83094 (October 15, 2024))
  - Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041) (90 Fed. Reg. 43560 (September 10, 2025))
- Moving trust (*i.e.*, include in contracts) to verify (*i.e.*, self, then third-party examination by DIBCAC or C3PAOs).

Fox Rothschild | Kiewit | MASSMAN CONSTRUCTION CO.

CMMC Program Levels



Level 1

Contractors handling Federal Contract Information (FCI)

Represents "Foundational" security practices

Level 2

Contractors processing, storing, or handling CUI as part of a DoD contract

Represents "Advanced" security practices

Level 3

Applicable to contractors processing, storing, or handling CUI associated with the most sensitive DoD programs

Fox Rothschild | Kiewit | MASSMAN CONSTRUCTION CO.

What is New? The Rollout Timeline

The Final 32 CFR Part 170 and 48 CFR rules have laid out key milestones for the requirement of CMMC compliance.

DEC. 16, 2024

32 CFR 170 Rule went into effect.

C3PAO Assessments Began.

NOV 10, 2025

Phase 1 Began:
Self-Assessment scores must be submitted to SPRS

C3PAO Assessments optional

NOV 10, 2026

Phase 2:
C3PAO Level 2 Assessments to be required for "applicable DoD solicitations and contracts as a condition of award.

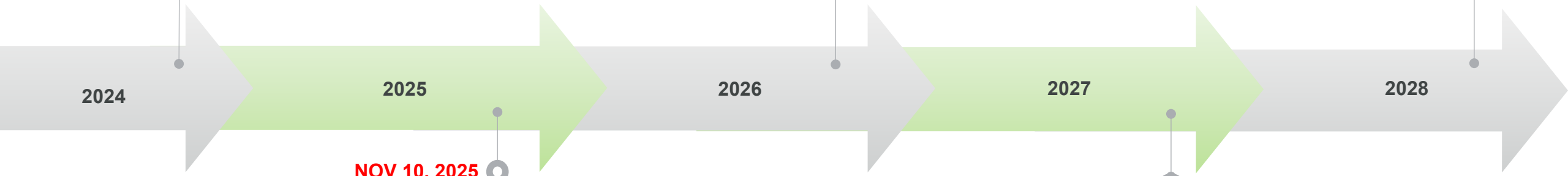
DIBCAC may conduct Level 3 assessments

NOV 10, 2027

Phase 3:
Level 2 Assessments with C3PAO Required for Contractors Given Option Period Extension.

NOV 10, 2028

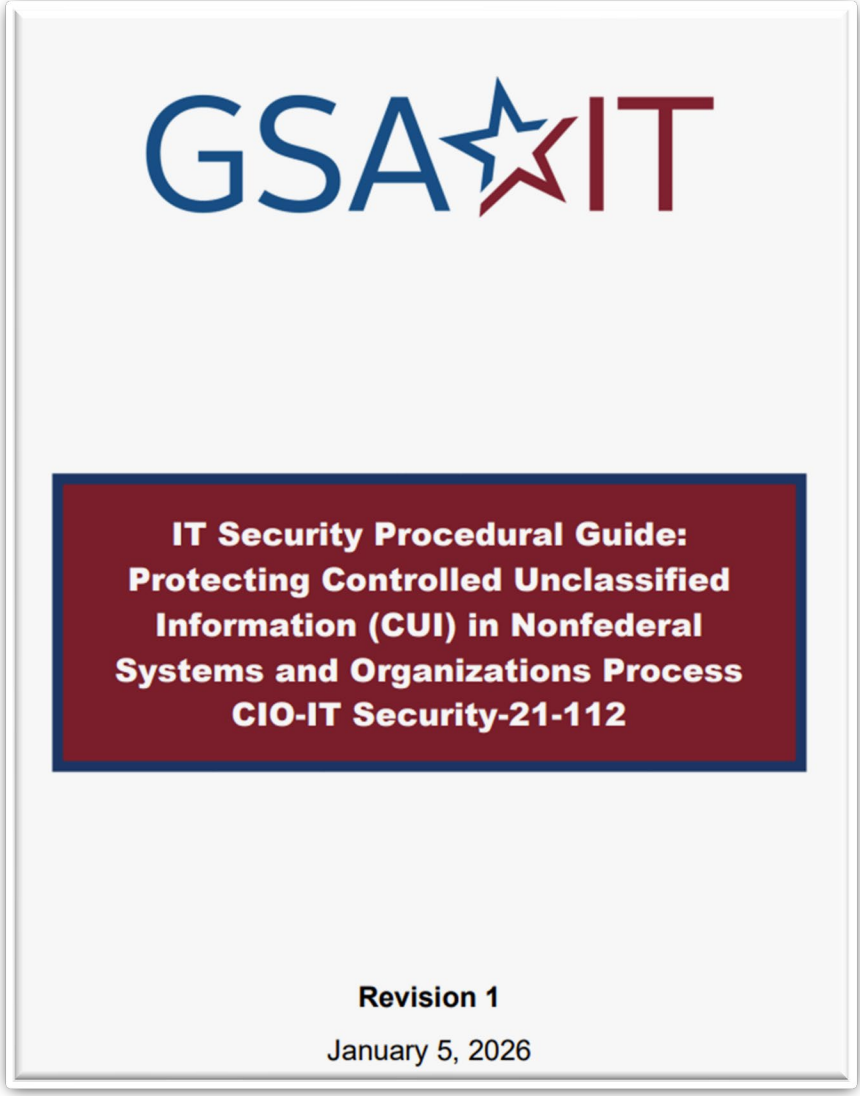
Phase 4: Full Implementation
All DoD Contracts Will Include CMMC Compliance Requirements.



Fox Rothschild | Kiewit | Massman Construction Co.

GSA Rolls Out Its Own CMMC

- On January 5, 2026, GSA published new cybersecurity requirements mirroring the CMMC
- Though styled as internal agency guidance, the document states contractors SHALL:
  - Comply with all of the security controls specified in NIST SP 800-171 rev3, select controls from NIST SP 800-172 rev3, and select controls from NIST SP 800-53 rev5
  - Engage in a five-step approval process, including third-party assessment and continued compliance monitoring
  - Comply with a strict one-hour cyber incident reporting requirement.



Fox Rothschild · Kiewit · Massman Construction Co.

How is implementation going?

- **Widespread Readiness Gaps**
  - As of October 2025, only 431 organizations had achieved a final CMMC Level 2 certification—representing just 0.5% of the roughly 80,000 companies the DoD/DoW estimates will require Level 2
- **Burden on Small Businesses**
  - Small business represent 74% of the Defense Industrial Base; the total cost of achieving Level 2 certification ranges from $50,000 to $400,000
- **C3PAO Capacity Bottleneck**
  - 103 accredited C3PAOs serving approximately 80,000 entities requiring CMMC Level 2 or Level 3

Step 1 – CMMC Level Selection

- On November 10, 2025, DOD solicitations began to specify the minimum CMMC Status required for award eligibility.
- CMMC Statuses:
  - Level 1 (Self) is a self assessment to secure FCI
  - Level 2 (Self) is a self assessment to secure CUI
  - Level 2 (C3PAO) requires the OSA to hire a C3PAO to conduct the assessment to secure CUI (beginning November 10, 2026)
  - Level 3 (DIBCAC) is a government assessment for the security of the most sensitive CUI

Step 2 – Scoping

- Prior to assessment, the CMMC Assessment Scope must be specified in accordance with the requirements of 32 CFR 170.19
- Level 1 Scoping
  - Information systems that process, store, or transmit FCI are in scope and must be assessed.
  - OSA's should consider people, technology, facilities, and External Service Providers within its environment.
- Levels 2 & 3 Scoping
  - Scoping is based on defined asset categories and their respective requirements at Tables 3 to 6 at 32 CFR 170.19.
    - CUI Assets (Levels 2 & 3)
    - Contractor Risk Managed Assets (Level 2)
    - Security Protection Assets (Levels 2 & 3)
    - Specialized Assets (Levels 2 & 3)

Step 3 – Assessment & Affirmation Level 1 (Self)

- Must comply with all 15 requirements of FAR 52.204-21
- Must submit affirmation of compliance into Supplier Performance Risk System (SPRS)
- To maintain CMMC Level 1, the assessment and affirmation must be repeated annually

Step 3 – Assessment and Affirmation Level 2 (Self) & Level 2 (C3PAO)

- Must comply with all 110 NIST SP 800-171 Rev. 2 security requirements
  - Self assessment or assessment by CMMC Third-Party Assessment Organization (C3PAO) depending on scope
- Must submit affirmation of compliance into SPRS annually
- CMMC status will be valid for three years
- Not all requirements need be met immediately
  - If minimum score is achieved (80% of maximum score) and certain critical requirements are met, OSA will receive CMMC Status Conditional Level 2.
  - All unmet requirements must be noted in a Plan of Action and Milestones (POA&M).
  - OSA is eligible for award but must meet all 110 security requirements within 180 days of receiving conditional status.

Fox Rothschild | Kiewit | MASSMAN CONSTRUCTION CO.

Step 3 – Assessment and Affirmation Level 3 (DIBCAC)

- Requires both Level 2 and Level 3 assessments
  - Must comply with all 110 NIST SP 800-171 R2 security requirements **AND** 24 selected requirements from NIST SP 800-172
- Assessment conducted by Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)
- Must submit affirmation of compliance into SPRS after each assessment and annually thereafter
- Level 2 and Level 3 assessments must be conducted every three years
- As with level 2, not all requirements need be met immediately
  - Unmet requirements must be addressed in a POA&M and met within 180 days of receiving conditional status

Step 4 – Flow-Down Requirements

- Subcontractors must also have a minimum a CMMC level based on the prime contractor's CMMC level

Prime Contractor Requirements	Minimum subcontractor requirement if the subcontractor will process, store, or transmit:	
	Federal Contract Information (FCI)	Controlled Unclassified Information (CUI)
Level 1 (Self) Level 2 (Self) Level 2 (C3PAO) Level 3 (DIBCAC)	Level 1 (Self) Level 1 (Self) Level 1 (Self) Level 1 (Self)	N/A Level 2 (Self) Level 2 (C3PAO) Level 2 (C3PAO)

Cyber Security Maturity Model Certification (CMMC) Program, 89 Fed. Reg. 83092 (October 15, 2024)

Practical advice

- **CMMC Level in Solicitation**: The CO must include in the solicitation the CMMC level that must be met by each contractor information system that processes, stores, or transmits FCI or UCI.
- **CMMC Unique Identifier (UID)**: Each CMMC assessment of contractor information systems entered into SPRS will be assigned a ten-character UID. Contractors must provide with their proposals the UIDs for each information system to be used in the performance of the contract.
- **Affirming Official**: Contractors should maintain an "affirming official" with the authority to affirm the contractor's continuing compliance with the CMMC program.
- **Subcontractor Affirmation of Compliance**: Prior to subcontract award, and annually thereafter, subcontractors must complete an affirmation of compliance with the requisite subcontractor CMMC level. Prime contractors are responsible for subcontractor compliance.
- **Only Store on CMMC-Assessed Systems:** Only store, process, or transmit FCI or CUI in CMMC-assessed information systems of the appropriate level.

Fox Rothschild | Kiewit | MASSMAN CONSTRUCTION CO.

Potential Risks of Noncompliance

DOD Memo – June 16, 2022

- *"Contractual Remedies to Ensure Contractor Compliance with DFARS 252.204-7012 for contracts not subject to DFARS 252.204-7020…."*
- *"Failure to have or make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of requirements. Remedies for such breach may include:*
  - *Withholding progress payments;*
  - *Foregoing remaining contract options;*
  - *And potentially terminating the contract in part or in whole."*

False Claims Act Implications

- DOJ is increasing its utilization of the False Claims Act (FCA) to address federal contractors' cybersecurity weaknesses.
- In FY2025, DOJ recovered $52 million in cybersecurity fraud settlements.
- Deputy Assistant Attorney General Brenna E. Jenny at the 2026 American Conference Institute's Advanced Forum on False Claims and Qui Tam Enforcement:
  - Cyber-fraud cases are "**not about data breaches**," but are instead "**premised on misrepresentations**."

Fox Rothschild | Kiewit | MASSMAN CONSTRUCTION CO.

False Claims Act Implications

- CMMC draws increased attention to cybersecurity compliance
  - Whistleblower incentives to disclose noncompliant systems and practices.
  - Bid/Proposal submission with non-compliant or non-existent System Security Plan (SSP) or Plan of Action and Milestones (POA&M).
  - C-Suite Tension (CEO/CISO/CIO) – Cost/Risk Mitigation Trade-Offs
- But is also an opportunity to clearly demonstrate compliance
  - The requirement for a third-party assessment of a contractors' cybersecurity infrastructure provides credible, independent evidence of compliance.
  - Compliance with CMMC should be used to seek improved terms from the insurance marketplace where possible

Fox Rothschild | Kiewit | MASSMAN CONSTRUCTION CO.

Risks of Noncompliance

- *United States et al v. Morsecorp Inc., et al* (Mar. 2025)
  - $4.6 million settlement for allegedly failing to implement NIST cybersecurity controls, failing to report noncompliance, and using an unvetted company to host emails without ensuring the company met Federal Risk and Authorization Management Program (FedRAMP) requirements.
- *United States ex rel. Doe v. Raytheon Co. et al* (Apr. 2025)
  - $8.4 million settlement to resolve FCA whistleblower suit alleging misrepresentation of cybersecurity compliance deficiencies, including the use of noncompliant internal systems to handle protected information.

Kiewit's Journey to CMMC Compliance

Lessons From the Road

PRE-2022 | 2022–2023 | LATE 2023 | 2024–2025 | FEB 2026

Foundation

- Stood up GCC High tenant for DFARS compliance
- Navigated real friction: isolated from commercial environment, duplicate licenses, restricted operations

Lesson: Client audits were our best ally — gave us external validation when pushing back on internal resistance.

Our Journey to CMMC Compliance

Lessons From the Road

PRE-2022 | 2022–2023 | LATE 2023 | 2024–2025 | FEB 2026

Foundation

- Stood up GCC High tenant for DFARS compliance
- Navigated real friction: isolated from commercial environment, duplicate licenses, restricted operations

Lesson: Client audits were our best ally — gave us external validation when pushing back on internal resistance.

GRC Readiness

- GRC team dedicated significant cycles to understanding CMMC — what it meant, timing, and our exposure
- Mapped controls gap; determined where we stood against NIST 800-171

Lesson: Investing in understanding the regulation before building anything saved us from expensive wrong turns.

Our Journey to CMMC Compliance

Lessons From the Road

PRE-2022 | 2022–2023 | LATE 2023 | 2024–2025 | FEB 2026

Foundation

- Stood up GCC High tenant for DFARS compliance
- Navigated real friction: isolated from commercial environment, duplicate licenses, restricted operations

Lesson: Client audits were our best ally — gave us external validation when pushing back on internal resistance.

GRC Readiness

- GRC team dedicated significant cycles to understanding CMMC — what it meant, timing, and our exposure
- Mapped controls gap; determined where we stood against NIST 800-171

Lesson: Investing in understanding the regulation before building anything saved us from expensive wrong turns.

Enclave Decision

- Chose a CUI enclave as our compliance path — scoped and isolated rather than lifting the whole enterprise
- Engaged an MSSP; a significant shift for an organization that handles most IT in-house

Lesson: Scoping discipline is everything. The enclave decision cut our compliance surface in half.

Our Journey to CMMC Compliance

Lessons From the Road

PRE-2022 — Foundation

- Stood up GCC High tenant for DFARS compliance
- Navigated real friction: isolated from commercial environment, duplicate licenses, restricted operations

Lesson: Client audits were our best ally — gave us external validation when pushing back on internal resistance.

2022–2023 — GRC Readiness

- GRC team dedicated significant cycles to understanding CMMC — what it meant, timing, and our exposure
- Mapped controls gap; determined where we stood against NIST 800-171

Lesson: Investing in understanding the regulation before building anything saved us from expensive wrong turns.

LATE 2023 — Enclave Decision

- Chose a CUI enclave as our compliance path — scoped and isolated rather than lifting the whole enterprise
- Engaged an MSSP; a significant shift for an organization that handles most IT in-house

Lesson: Scoping discipline is everything. The enclave decision cut our compliance surface in half.

2024–2025 — Build & Prepare

- Enclave environment largely complete by end of 2024
- 2025 focused on business processes, evidence organization, and assessment readiness — not the technology

Lesson: The tech was the easy part. Evidence collection and process documentation took far longer than expected.

FEB 2026

Our Journey to CMMC Compliance

Lessons From the Road

✓ L2 Certified Feb 2026

PRE-2022 | 2022–2023 | LATE 2023 | 2024–2025 | FEB 2026

Foundation

- Stood up GCC High tenant for DFARS compliance
- Navigated real friction: isolated from commercial environment, duplicate licenses, restricted operations

Lesson: Client audits were our best ally — gave us external validation when pushing back on internal resistance.

GRC Readiness

- GRC team dedicated significant cycles to understanding CMMC — what it meant, timing, and our exposure
- Mapped controls gap; determined where we stood against NIST 800-171

Lesson: Investing in understanding the regulation before building anything saved us from expensive wrong turns.

Enclave Decision

- Chose a CUI enclave as our compliance path — scoped and isolated rather than lifting the whole enterprise
- Engaged an MSSP; a significant shift for an organization that handles most IT in-house

Lesson: Scoping discipline is everything. The enclave decision cut our compliance surface in half.

Build & Prepare

- Enclave environment largely complete by end of 2024
- 2025 focused on business processes, evidence organization, and assessment readiness — not the technology

Lesson: The tech was the easy part. Evidence collection and process documentation took far longer than expected.

Certified

- Level 2 third-party C3PAO certification achieved
- Now sustaining: continuous monitoring, annual affirmation, sub compliance requirements

Lesson: Certification is the beginning of the program, not the end of the project.

If You're Just Getting Started: What I Wish I Had Known

Starting Point Guide

01 Answer This First: Do You Have CUI?

Don't assume. Review every DoD contract for DFARS 252.204-7012 clauses. Read your drawings, specs, and submittals through the lens of the DoD CUI Registry. "We're just a contractor" is not a scoping answer.

Common mistake: assuming field execution subs are exempt.

If You're Just Getting Started: What I Wish I Had Known

Starting Point Guide

01 Answer This First: Do You Have CUI?

Don't assume. Review every DoD contract for DFARS 252.204-7012 clauses. Read your drawings, specs, and submittals through the lens of the DoD CUI Registry. "We're just a contractor" is not a scoping answer.

⚑ *Common mistake: assuming field execution subs are exempt.*

02 Get a Real Gap Assessment — Not a Checklist

A spreadsheet self-assessment will flatter you. Hire an independent assessor to evaluate actual control implementation and document evidence. Your SPRS score should reflect reality — it's now a legal attestation.

⚑ *Common mistake: confusing a policy document with a control.*

If You're Just Getting Started: What I Wish I Had Known

Starting Point Guide

01 Answer This First: Do You Have CUI?

Don't assume. Review every DoD contract for DFARS 252.204-7012 clauses. Read your drawings, specs, and submittals through the lens of the DoD CUI Registry. "We're just a contractor" is not a scoping answer.

Common mistake: assuming field execution subs are exempt.

02 Get a Real Gap Assessment — Not a Checklist

A spreadsheet self-assessment will flatter you. Hire an independent assessor to evaluate actual control implementation and document evidence. Your SPRS score should reflect reality — it's now a legal attestation.

Common mistake: confusing a policy document with a control.

03 Scope Ruthlessly, Then Protect the Boundary

The smaller your CUI enclave, the faster and cheaper your path to certification. Isolate systems that touch CUI. Don't let project convenience expand the boundary — every addition multiplies your compliance burden.

Common mistake: letting project teams add tools mid-assessment.

If You're Just Getting Started: What I Wish I Had Known

Starting Point Guide

01 Answer This First: Do You Have CUI?

Don't assume. Review every DoD contract for DFARS 252.204-7012 clauses. Read your drawings, specs, and submittals through the lens of the DoD CUI Registry. "We're just a contractor" is not a scoping answer.

Common mistake: assuming field execution subs are exempt.

02 Get a Real Gap Assessment — Not a Checklist

A spreadsheet self-assessment will flatter you. Hire an independent assessor to evaluate actual control implementation and document evidence. Your SPRS score should reflect reality — it's now a legal attestation.

Common mistake: confusing a policy document with a control.

03 Scope Ruthlessly, Then Protect the Boundary

The smaller your CUI enclave, the faster and cheaper your path to certification. Isolate systems that touch CUI. Don't let project convenience expand the boundary — every addition multiplies your compliance burden.

Common mistake: letting project teams add tools mid-assessment.

04 Plan for 18 Months, Not 18 Weeks

Gap analysis → remediation → SSP documentation → pre-assessment → C3PAO scheduling → formal assessment. Each step takes longer than expected. C3PAO slots are already booking into late 2026. Start the clock now.

Common mistake: treating CMMC as an IT project with a deadline.

If You're Just Getting Started: What I Wish I Had Known

Starting Point Guide

01 Answer This First: Do You Have CUI?

Don't assume. Review every DoD contract for DFARS 252.204-7012 clauses. Read your drawings, specs, and submittals through the lens of the DoD CUI Registry. "We're just a contractor" is not a scoping answer.

Common mistake: assuming field execution subs are exempt.

02 Get a Real Gap Assessment — Not a Checklist

A spreadsheet self-assessment will flatter you. Hire an independent assessor to evaluate actual control implementation and document evidence. Your SPRS score should reflect reality — it's now a legal attestation.

Common mistake: confusing a policy document with a control.

03 Scope Ruthlessly, Then Protect the Boundary

The smaller your CUI enclave, the faster and cheaper your path to certification. Isolate systems that touch CUI. Don't let project convenience expand the boundary — every addition multiplies your compliance burden.

Common mistake: letting project teams add tools mid-assessment.

04 Plan for 18 Months, Not 18 Weeks

Gap analysis → remediation → SSP documentation → pre-assessment → C3PAO scheduling → formal assessment. Each step takes longer than expected. C3PAO slots are already booking into late 2026. Start the clock now.

Common mistake: treating CMMC as an IT project with a deadline.

05 Build the Program Around People, Not Tools

The SSP requires a named owner for each of 110 controls. That means HR, Legal, Facilities, and Operations are part of your compliance program whether they know it yet or not. Executive sponsorship is not optional.

Common mistake: assigning all 110 controls to the CISO.

If You're Just Getting Started: What I Wish I Had Known

Starting Point Guide

01 Answer This First: Do You Have CUI?

Don't assume. Review every DoD contract for DFARS 252.204-7012 clauses. Read your drawings, specs, and submittals through the lens of the DoD CUI Registry. "We're just a contractor" is not a scoping answer.

Common mistake: assuming field execution subs are exempt.

02 Get a Real Gap Assessment — Not a Checklist

A spreadsheet self-assessment will flatter you. Hire an independent assessor to evaluate actual control implementation and document evidence. Your SPRS score should reflect reality — it's now a legal attestation.

Common mistake: confusing a policy document with a control.

03 Scope Ruthlessly, Then Protect the Boundary

The smaller your CUI enclave, the faster and cheaper your path to certification. Isolate systems that touch CUI. Don't let project convenience expand the boundary — every addition multiplies your compliance burden.

Common mistake: letting project teams add tools mid-assessment.

04 Plan for 18 Months, Not 18 Weeks

Gap analysis → remediation → SSP documentation → pre-assessment → C3PAO scheduling → formal assessment. Each step takes longer than expected. C3PAO slots are already booking into late 2026. Start the clock now.

Common mistake: treating CMMC as an IT project with a deadline.

05 Build the Program Around People, Not Tools

The SSP requires a named owner for each of 110 controls. That means HR, Legal, Facilities, and Operations are part of your compliance program whether they know it yet or not. Executive sponsorship is not optional.

Common mistake: assigning all 110 controls to the CISO.

06 Your Subs Are Part of Your Compliance Posture

CUI you share with a sub is CUI you're responsible for. Flow-down clauses are legally required but don't protect you operationally. Know your subs' readiness before you share sensitive data — not after.

Common mistake: assuming your contract language is enough.

Thank you!