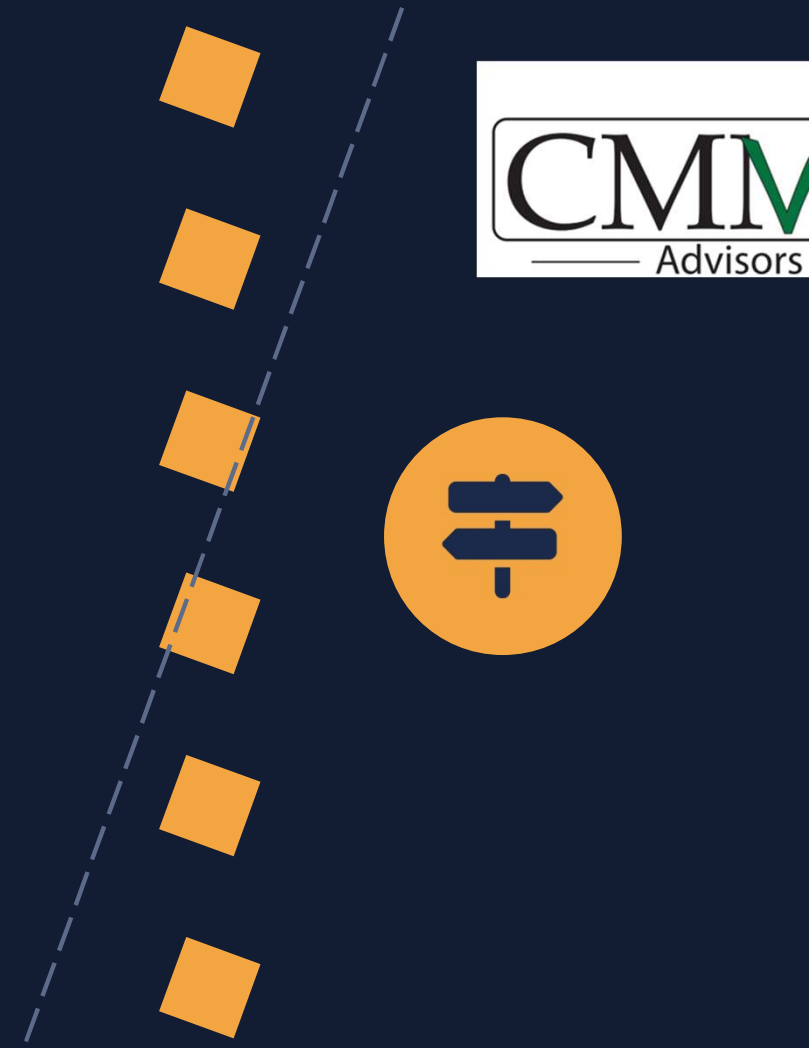
PNW – CMMC · AUGUST 2026

A CMMC Roadmap & The Resources Actually Required

Find your fork in the CMMC road — then shop for what you actually need, not everything on the market.

Jerry Leishman (CEO)

CMMC Advisors | cmmcadvisors.com



YOUR PRESENTER

Jerry Leishman

CEO, CMMC Advisors · Vice Chair, CMMC Industry Standards Council

Presidential Volunteer Service Award, 2020

Jerry Leishman is a trusted advisor to in-house counsel, compliance officers, and executive leadership, helping organizations confidently navigate complex regulatory, legal, and contractual landscapes. As the CEO of **CMMC Advisors**, he leads efforts to support Defense and Critical Infrastructure suppliers of all sizes in achieving cybersecurity maturity and compliance.

Previously, Jerry served as Executive Vice President and National Security & Compliance Director at **CORTAC Group**, following a 15-year career at **Microsoft** where he held various leadership roles in public sector, security, and compliance.

Nationally recognized for his contributions, Jerry was an original member of the **CMMC Accreditation Body (CMMC-AB) Standards Workgroup** and received the **Presidential Volunteer Service Award** for his service. He currently serves as **Vice Chair of the CMMC Industry Standards Council (CISC)** and **Co-Chair of the Software for Defense non-profit**. He holds multiple certifications including **Certified CMMC Assessor (CCA)**, **Certified CMMC Professional (CCP)**, **Provisional Assessor (PA)**, and **Registered Practitioner (RP)**.

A frequent national speaker, Jerry advises Defense Industrial Base (DIB) executives on cybersecurity, DFARS, and CMMC readiness — empowering leadership to understand their strategic roles across government, partner, and supplier ecosystems. He maintains deep ties with the CMMC community and technology leaders supporting secure and resilient defense supply chains.

WHAT WE'LL COVER

Agenda

01 **The Business Stakes**
Why picking the wrong resource is an expensive, personal risk.

02 **The CMMC Program Journey**
The five milestones from first assessment to certification.

03 **The Questions You Walk In With**
The four things every OSC in this room is actually wondering.

04 **The Roadmap: Four Forks in the Road**
Where you are, and what category of help matches each fork.

05 **Choosing Your Technology Platform Stack**
All Cloud, Hybrid, or On-Premise — weighed against cost and CUI needs.

06 **What You Don't Know to Ask Yet**
Diagnostic signals that tell you which fork you're really on.

07 **Avoiding the Impulse Buy**
Real cost ranges, a real case study, and how to stop overspending.

08 **Your Next Step**
Turning today's diagnosis into a short, evaluable list.

SETTING THE STAGE

Who's in This Room Today

You're a small or mid-size Defense Industrial Base supplier. Your Department of War contracts require you to meet NIST SP 800-171 R2 — and eventually demonstrate it through CMMC. You're not a compliance department. You're the business owner, the project lead, or the person who got handed this.

Small & Mid-Size

Not a Fortune 500 compliance department — lean teams wearing many hats.

NIST 800-171 R2

Required to protect CUI to meet Dept. of War contract flow-downs.

Business Owners

Making the call, not just implementing someone else's decision.

WHY THIS ROADMAP MATTERS

What's Actually at Stake

This isn't an IT checkbox. For the owner or project lead in this room, CMMC touches revenue, legal exposure, and trust — which is exactly why picking the wrong resource is an expensive mistake.

Business & Revenue Loss

Contract disqualification means lost bids and lost revenue on work you already do today.

Legal Liability

Misrepresenting your compliance status carries real False Claims Act exposure — for the business and for you personally.

Trust Erosion

Primes and government customers are watching how seriously you take security. That reputation is hard to rebuild.

It Lands on the Owner

As the business or project lead, you're the one accountable when compliance falls short — not a distant IT department.

THE PROBLEM

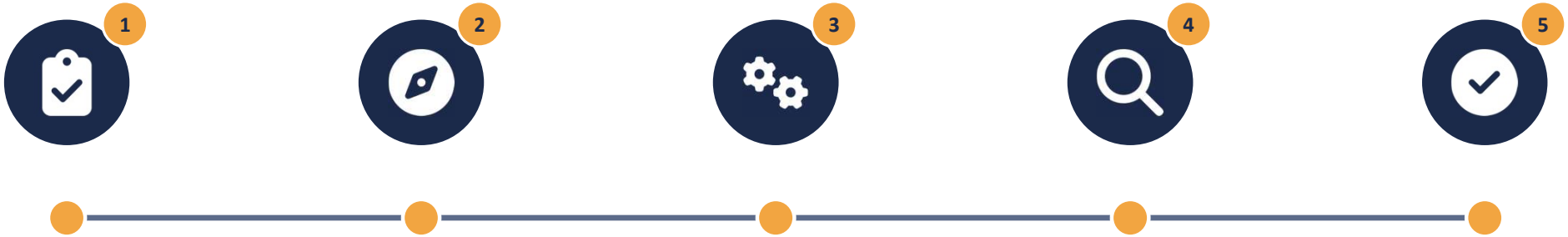
Most contractors try to shop the entire market at once — and freeze.

Advisors, RPOs, MSPs, MSSPs, GRC platforms, C3PAOs, GCC High migrations — it all lands in your inbox at once. Without a way to sort it, every option looks equally urgent, and none of them are.

THE BIG PICTURE

The CMMC Program Journey

Five milestones from first assessment to certification — the road ahead, regardless of which fork you're on today.



Gap / Self-Assessment

Baseline vs. 110 controls

Remediation Planning

Right-sized roadmap

Implementation

Validation, Deployment, & Change Managemtn

Pre / Mock Assessment

320 objectives, evidence

Certification & Maintain

Self / C3PAO, ongoing

QUESTIONS AN OSC WALKS IN WITH

What You're Actually Wondering

Where am I on the CMMC roadmap — and what resource helps me take the next step?

I don't know where to start. Who or what do I even need first?

Do I need an advisor, an MSP, a tool, a new platform — or some combination?

How do I avoid buying things I don't need yet?

THE FRAMEWORK

The CMMC Roadmap: Four Forks in the Road

Every OSC's journey runs through some version of these four forks. Find the one you're standing at, and the market shrinks from everything to one category.

Starting Direction

Advisor / RPO

Tracking & Evidence

GRC Tool

CUI Boundary / Right Systems

Right Architecture/ Right Resources/ Right Plan/Right Applications

Managed Operations

MSP / Specialist

FORK 1 OF 4 · STARTING DIRECTION

I Don't Know Where to Start

THE SIGNAL

“I don’t know where to start.”

You haven’t scoped your environment, you’re not sure what CUI you touch, and every vendor call sounds like the first step. That uncertainty itself is the signal.

WHAT ACTUALLY HELPS

An Advisor or RPO

Choose a direction, not a product. A Registered Practitioner Organization (RPO) or advisor helps you educatie your stakeholders, scope your environment, understand your CUI boundary, know industry solutions, and sequence the work — before you buy anything.

Buying a tool here just gives you an expensive place to store confusion.

FORK 2 OF 4 · TRACKING & EVIDENCE

I Have a Team, But I'm Chasing Evidence

THE SIGNAL

“We know what to do — we just can’t keep track of it.”

You have people assigned to the work. Controls are being implemented. But your evidence lives in a dozen spreadsheets, your POA&M is stale by the time you open it, control validation is unknown, and nobody can answer “what’s our SPRS score right now” without a scramble.

WHAT ACTUALLY HELPS

A GRC Platform

This is a tooling problem, not a staffing problem. A GRC platform centralizes your SSP, POA&M, policy, procedures, evidence, and ongoing control validation assurance so your team's effort is visible and defensible — instead of trapped in files.

Adding headcount here treats the symptom, not the cause.

FORK 3 OF 4 · CUI DISCOVERY & SPECIFIC OBJECTIVES

I Have One Objective I Can't Solve by Changing Behavior

THE SIGNAL

“I know exactly what’s blocking me — and training won’t fix it.”

Maybe it's finding where CUI actually lives across your file shares. Maybe it's a boundary problem, or an email environment that isn't GCC High. It's a specific, technical objective — not a general capability gap.

WHAT ACTUALLY HELPS

The Right Tools

Choose a solution built for your specific need and cost optimized — data discovery, boundary enforcement, supplier file exchange, or GCC High migration — rather than an oversized platform packed with unneeded features and costs. That said, this decision still shapes daily workflows and user adoption, so weigh both your current needs and the end-user experience before committing.

This is the one fork where a platform or point solution COULD BE genuinely the right answer or genuinely wrong if the requirements are not understood.

FORK 4 OF 4 · MANAGED OPERATIONS

I Don't Have the Capacity to Run This Day to Day

THE SIGNAL

“We know what ‘right’ looks like. We just can’t staff it.”

Your controls are designed, your tooling may already be in place — but monitoring, patching, log review, and incident response need daily attention your team doesn't have hours for. You must maintain compliance annually and keep the system operationally compliant.

WHAT ACTUALLY HELPS

An MSP or Compliance Specialist

The right fit depends on your scope — your CUI boundary, your enclave design, your headcount — not on who pitched loudest.

Match the service provider to the operational footprint you actually have and what is the highest and best use of your internal resources.

This is a scope conversation first, a vendor conversation second.

A DECISION INSIDE EVERY FORK

Choosing Your Technology Platform Stack

Whichever fork you're on, most roadmaps eventually hit this question: All Cloud, Hybrid, or On-Premise. Weigh it against your prior investments and your ERP/CAD footprint — not just sticker price.

Consideration	All Cloud	Hybrid	On-Premise
Short-term fit	Fastest to stand up; minimal upfront infrastructure spend	Moderate speed; priority CUI workloads move to cloud first	Slowest to deploy; capex required before go-live or Turnkey CMMC Ready CUI On-premise enclave
Long-term fit	Scales easily; provider maintains the FedRAMP-authorized boundary	Flexible; capacity shifts to cloud incrementally as needs grow	Fixed capacity; hardware refresh every 3–5 years
Prior Infrastructure investments	Existing on-prem hardware becomes a sunk cost	Reuses current servers/network for non-CUI workloads	Fully leverages hardware and facility already in place
Applications, if CUI Needs (e.g. ERP / CAD)	Needs a FedRAMP-authorized SaaS ERP/CAD or GCC High/gov cloud wrapper	Legacy ERP/CAD stays on-prem inside a defined CUI enclave	Full control over ERP/CAD data flow and CUI boundary
Licensing	Subscription / consumption-based; scales with seats or usage	Mixed subscription and perpetual licenses across environments	Perpetual licenses plus annual maintenance & support
Implementation cost	Lower upfront; higher recurring subscription cost	Moderate upfront; integration work adds cost	Higher upfront capex for hardware, facility, and setup
Operational cost	Provider handles patching, monitoring, operations	Shared responsibility; still needs in-house IT for on-prem piece	Requires IT/security staff day to day
Sample Solutions	Gov CSPs - Microsoft GCC/GCCH, Azure Gov, AWS Gov, Google Gov Workspaces	GCCH/Google Workspace, Prevail, Octa, Virtu, CMMC Advisors System In A Box (CMMC Ready)	Windows, Linux, Fortinet, Palo Alto, VMWare, CMMC Advisors System In A Box (CMMC Ready)

WHAT YOU DON'T KNOW TO ASK YET

Match Your Symptom to Your Fork

What you're experiencing	The likely fork	The resource category
“I genuinely don't know where to start.”	**Starting Direction**	**Advisor / RPO**
“We have a team, but we're chasing tracking and evidence.”	**Tracking & Evidence**	**GRC Tool**
“Multiple vendors tell me their solution solves CMMC, how do I know.”	**CUI Boundary / Right Systems**	**The Right Product**
“We lack the internal capacity to run it day to day.”	**Managed Operations**	**MSP / Specialist**

BUY SECOND, NOT FIRST

How to Avoid the Impulse Buy

Diagnose your fork first

Use the signals, not the sales call, to decide which category you're shopping in.

Don't buy a platform for a staffing gap

A GRC tool won't run your SOC. Match the purchase to the actual constraint.

Don't hire an MSP for a one-time objective

A CUI discovery project doesn't need a managed services contract.

Match category to fork — not the loudest pitch

The most persuasive vendor in the room isn't necessarily solving your problem.

Shop Around— Talk to your trusted advisor for qualified vendors

Tool and services prices vary dramatically. Shop for right sized and cost optimized solutios

GROUNDING THE DECISION IN REAL NUMBERS

What This Actually Costs: Year 1

Ballpark ranges from real CMMC Level 2 engagements — knowing your fork tells you which lines actually apply to you.

CUI Discovery, Gap Assessment & Planning	**$15,000 – $50,000**
Gap Remediation, Implementation & Tools	**$25,000 – $300,000**
Pre-Assessment & Mock Verification	**$5,000 – $20,000**
C3PAO Assessment	**$30,000 – $80,000**
Total Year 1 Investment	**$75,000 – $450,000+**
Year 2–3 Ongoing / Annual Affirmation	**$50,000 – $150,000+ per year**

REAL EXAMPLE

A defense manufacturer's MSP recommended a full GCC High migration that wasn't required for their scope. Proper re-scoping avoided $300K in unnecessary spend — while still meeting all 110 required controls.

WHY IT MATTERS FOR YOUR DECISIONS

From an Overwhelming Market to a Short List You Can Evaluate

WITHOUT A ROADMAP

Every advisor, MSP, and tool looks equally urgent. You evaluate the whole market at once — and freeze, or buy on instinct.

WITH A ROADMAP

You diagnose your fork, then evaluate a short list within one category. That's the difference between an informed purchase and an impulse buy.

YOUR NEXT MOVE

Evaluate at the Category Level

1

Identify your fork

Use today's diagnostic signals — not a sales pitch — to name where you stand.

2

Shortlist within one category

Two or three options in the ONE category that matches your fork. Not the whole market.

3

Ask category-specific questions

For RPO: what are key success factors across my CMMC journey?

For a GRC tool: how does evidence map to assessment objectives?

For an MSP: what's your CUI enclave design and shared responsibility matrix?

4

Reassess at your next milestone

Your fork changes as your program matures. Revisit the roadmap, don't set it once and forget it.

You can be past Fork 1 and still land back on Fork 2 a year later — that's normal, not a failure.

YOUR PRESENTER · YOUR NEXT STEP

Find Your Fork in the CMMC Road

Jerry Leishman, CMMC Advisors — someone who helped write the standard. There's no one-size-fits-all provider, so shop for what you actually need, not everything on the market.

Not sure which fork you're on?

Bring your situation to us after this session — we'll help you diagnose it in 20 minutes.

Ready to shortlist?

We can point you to the right category of provider — vendor-neutral, based on your fork.

Want the full picture?

Reach out at cmmcadvisors.com to talk through your roadmap end to end.

THE BOTTOM LINE FOR LEADERSHIP

CMMC isn't an IT project with a deadline. It's a strategic business decision.

It has direct implications for revenue, competitive position, and your long-term standing as a defense supplier. Organizations that act early control cost, timing, and risk. Those who wait accept whatever terms the deadline imposes.

The time to act is before the contract is on the line.

Questions?

Jerry Leishman | CMMC Advisors | cmmcadvisors.com

Thank You

Find your fork in the CMMC road —
then shop for what you actually need.

Jerry Leishman

CMMC Advisors | cmmcadvisors.com

Jerryleishman@cmmcadvisors.com