fellsway

CMMC FAQ

For Firearms, Defense, and Government-Adjacent Manufacturers

Be compliant. Be resilient. Be ready.

fellswaygroup.com

SECTION 1

Why This FAQ Matters

CMMC isn't an IT issue. It's a business decision.

For firearms-sector and defense-adjacent manufacturers, CMMC affects revenue, contract eligibility, legal exposure, prime relationships, and your competitive position. The companies treating it as a checkbox are losing ground. The ones treating it as a strategic posture are winning new business.

This FAQ pulls together the questions and answers geared towards executives, legal, finance, and IT during our recent webinar on CMMC for the firearms and defense supply chain. It's structured for two readers: leadership scanning for revenue, risk, and decision points, and the IT or program owner who has to implement and manage their company's CMMC program.

What's the single most important takeaway?

CMMC follows the data, not just the contract language. If you handle Controlled Unclassified Information, your obligations are already in motion, whether you've formally addressed them or not. The companies that move now protect revenue. The ones that wait pay more, in cost and in lost contracts.

Where to start: If you're not sure whether CMMC applies to you, what level you need, or whether your current program will hold up, Fellsway's complimentary 60-minute CMMC Readiness Workshop is the no-commitment way to get a clear answer.

Schedule your free workshop

SECTION 2

CMMC Basics and Applicability

What is CMMC?

Cybersecurity Maturity Model Certification. It's the Department of War framework that determines whether a company can hold or pursue contracts involving sensitive federal information. It replaces self-assessment with third-party validation for most defense contractors handling CUI.

What's the difference between Level 1, Level 2, and Level 3?

Level 1

Covers Federal Contract Information (FCI) and is self-assessed.

Level 2

Covers Controlled Unclassified Information (CUI) and requires either a self-assessment or, for most contracts, a formal C3PAO assessment.

Level 3

Covers high-value CUI exposed to advanced persistent threats and is assessed by the DoW itself, or the DIBCAC.

Most firearms and defense-adjacent manufacturers handling technical drawings, specifications, or program data fall under Level 2. The level you need is determined by your contracts and the data you handle, not by company size.

What are FCI and CUI?

FCI

Information provided by or generated for the federal government under contract that isn't intended for public release. It's broad and low-stakes.

CUI

The sensitive category. It includes technical data, drawings, specifications, manufacturing instructions, and program-specific information that the government has marked for protection. For firearms manufacturers, CUI often shows up as drawings, tolerances, manufacturing processes, and ITAR-controlled technical data.

Does CMMC apply only to direct DoW contractors?

No. CMMC follows the data and the contract through the supply chain. If you supply a prime, sub-tier integrator, or another manufacturer feeding a DoD program, the obligations flow down to you. Many tier-two and tier-three suppliers are in scope without realizing it.

If we're a commercial firearms manufacturer, can CMMC still apply?

Yes. Federal law enforcement contracts, federally funded purchases, allied-nation programs through Foreign Military Sales (FMS), and components flowing into defense end-use can all trigger requirements. ITAR-controlled technical data adds another layer that often overlaps with CUI obligations.

Does CMMC follow the contract, the customer, or the data?

All three, with the data as the anchor. The contract sets the obligation. The customer (and their customer, and theirs) determines flow-down. The data is what defines scope. If CUI lives in your environment, you have an obligation, regardless of whether you've signed something that names it explicitly.

Which firearms-sector roles are commonly in scope?

- Component manufacturers, including barrels, receivers, triggers, and ammunition components
- CNC and precision machining shops feeding defense programs
- Coating, heat-treating, and finishing vendors handling marked drawings
- Optics, mounts, and accessory manufacturers
- Anyone handling technical data, drawings, or specifications tied to defense end-use
- Importers, exporters, and logistics providers with FMS exposure

SECTION 3

Contracts, Flow-Down Clauses, and CUI Scope

What are flow-down clauses?

Contractual obligations that pass from a prime contractor to its suppliers, and from those suppliers to their suppliers. If your customer is contractually obligated to protect CUI, the contract you signed with them likely requires you to do the same. Most companies inherit these obligations without reading them carefully.

Which DFARS clauses should we look for?

DFARS 252.204-7012
Safeguarding CUI and reporting cyber incidents

DFARS 252.204-7019
Notice of NIST SP 800-171 DoD assessment requirements

DFARS 252.204-7020
NIST SP 800-171 DoD assessment requirements

DFARS 252.204-7021
Contractor compliance with the CMMC framework requirement

Could we already be subject to cybersecurity obligations without realizing it?

Yes. This is the most common situation we see. Companies sign contracts containing flow-down language, perform under them for years, and only learn about the obligations when a prime asks for an SPRS score or an assessment date. The obligation began when the contract was signed.

What should we search for in our contracts?

"DFARS"

"252.204"

"NIST 800-171"

"Controlled Unclassified Information"

"CUI"

"Cybersecurity"
Combined with any reference to a federal customer or end-use

How does ITAR-controlled technical data relate to CUI for firearms manufacturers?

ITAR data is almost always CUI when it touches a defense contract. The two regimes overlap heavily for firearms and ammunition manufacturers. If you've already built ITAR controls around technical data, you have a head start on CMMC scope, but the documentation and evidence requirements are different and need to be addressed directly.

Why is defining the CUI boundary the first real step?

Every downstream decision (cost, timeline, tooling, training, vendor scope) flows from where CUI lives. Companies that skip this step end up with programs that protect too much (driving cost up) or too little (driving certification risk up). Get the boundary right first. Everything else gets cheaper and faster from there.

SECTION 4

Revenue at Risk and Competitive Position

Why should leadership treat CMMC as a revenue issue, not an IT issue?

Because the cost of inaction shows up on the revenue line, not the IT budget. Lost contracts, lost RFQ opportunities, lost preferred-supplier status. The CMMC investment is a fraction of the revenue it protects, but only if you can map the revenue accurately.

How do we calculate our CMMC-touched revenue?

Map your revenue across these streams. Most companies miss at least two of them on the first pass.

- Direct DoD contracts
- Prime and tier-one defense relationships
- Sub-tier work flowing into defense end-use
- FMS and allied-nation programs
- Federal law enforcement and federally funded work
- Commercial relationships with defense exposure
  Vendors who supply primes, even if you don't

Are primes asking about CMMC for new business only, or existing relationships too?

Both. New business is where the formal language shows up first. Existing relationships are where the quiet pressure happens. Primes are filtering their supplier base by readiness, and suppliers who can't answer the question are getting fewer RFQs without ever being formally cut.

What does "deselection" mean?

Quiet removal from preferred supplier rotation. You don't get a termination letter. You stop getting calls. By the time you notice, the work has shifted to a competitor who answered the readiness question first.

Can CMMC readiness create a competitive advantage?

Yes, and the window is narrower than most companies realize. Ready or certified suppliers are using CMMC posture in capabilities decks, RFQ responses, and pricing conversations right now. Once the supply chain is broadly certified, the advantage flattens. Companies moving in 2026 capture more of it than companies moving in 2027.

How long does the first-mover advantage last?

Eighteen to thirty-six months, depending on sub-sector. The faster the prime's certification timeline pulls forward, the shorter the window. Once your competitors are certified, certification becomes table stakes, not a differentiator.

SECTION 5

SPRS Scores, Self-Assessment, and Affirming Officials

What is SPRS?

The Supplier Performance Risk System. It's the DoD's online portal where contractors post their NIST SP 800-171 self-assessment score. Primes check SPRS scores when evaluating suppliers. A low or missing score is a red flag.

What's the maximum SPRS score, and can it be negative?

The maximum is 110, awarded when all 110 NIST SP 800-171 controls are fully implemented. Yes, the score can go negative. Each unimplemented control deducts points based on weighting, and partial implementation doesn't earn full credit. Negative scores are common for companies that haven't done the work yet.

Who's responsible for the SPRS score?

The contractor. Specifically, the affirming official, an executive who signs to confirm the score is accurate. This isn't an IT signature. It's a leadership representation to the federal government, with all the legal weight that implies.

Why is an inaccurate SPRS score a legal risk?

Because it's a representation made to win or hold federal contracts. If the score is overstated, even unintentionally, the company and the affirming official can face False Claims Act exposure. The DOJ's civil cyber-fraud initiative has made enforcement of inaccurate cybersecurity claims an active priority.

What if our MSP or IT provider calculated the score and we're not sure it's right?

This is one of the most common scenarios we see. An MSP runs a tool, produces a number, and the affirming official signs it. The problem: SPRS scoring requires judgment about scope, control implementation, and evidence, and most MSPs aren't equipped to make those judgments at the level CMMC requires.

⚠ If you're not sure, get an independent review before you affirm anything else. The cost of validating a score is a fraction of the cost of defending an overstated one.

How often should the score be reviewed?

Quarterly at minimum, and any time your environment changes materially: new systems, new vendors, new contracts, new CUI flows, or staff turnover in roles that own controls. SPRS isn't a one-time number. It moves with your environment.

What should leadership ask before signing?

- What scope did this score cover? Is it the full environment or a subset?
- What evidence supports each control's score?
- Who reviewed the methodology, and were they independent of who scored it?
- When was the score last updated, and what's changed since then?
- Has anything been overstated to look better to a customer?

Why isn't "let me check with IT" a governance model?

Because the affirming official is signing for the company, not for IT. Delegating the question to IT delegates the answer, but not the liability. Leadership needs to understand the score well enough to defend it.

SECTION 6

False Claims Act, Legal Exposure, and Governance

Why does the False Claims Act keep coming up in CMMC conversations?

Because cybersecurity claims made to win federal contracts are claims under the FCA. If a company misrepresents its cybersecurity posture (in proposals, certifications, SPRS scores, or contract performance), the misrepresentation can become the basis for an FCA action.

Does FCA exposure require intentional fraud?

No. The FCA's "knowingly" standard covers actual knowledge, deliberate ignorance, and reckless disregard for the truth. A company that signs an SPRS affirmation without verifying the underlying score can be acting with reckless disregard, even without intent to deceive.

What does "reckless disregard" mean in practice?

Signing without checking. Affirming a score because IT said it was right, without independent verification. Inheriting a number from a predecessor and continuing to affirm it without review. The legal standard doesn't require malice. It requires you to have taken reasonable steps to know the truth.

Could company leaders or affirming officials face personal exposure?

Yes. The FCA allows for individual liability, and recent enforcement has named officers who signed cybersecurity certifications. This is a real reason to make sure the affirming official understands what they're signing and has independent confidence in the underlying assessment.

How do qui tam (whistleblower) actions work?

Private parties (often current or former employees) can file FCA suits on behalf of the government. If the case succeeds, the whistleblower gets a percentage of the recovery. Cyber-related qui tam filings have grown substantially in the last three years. Disgruntled IT staff who believe a score was overstated are a common source.

When should legal and finance be brought into the conversation?

Day one. CMMC is a legal exposure question and a finance allocation question, not just an IT project. Companies that bring legal and finance in late end up restructuring decisions that should have been made up front, at higher cost.

What goes wrong when CMMC is delegated only to IT or an MSP?

- Scope decisions get made without business context, resulting in over-protected (expensive) or under-protected (risky) environments
- Documentation gets written in IT language, not in language an assessor or attorney can defend
- Affirming officials sign without understanding what they're signing
- Legal exposure isn't surfaced until it's too late to address quietly
- The MSP makes early architectural decisions that don't survive C3PAO scrutiny

What should sit with each role?

Executive Sponsor
Owns the outcome and accountability

Legal
Owns representations, contract review, and FCA exposure

Finance
Owns cost categorization, allowability, and ROI framing

IT and MSP
Own technical implementation

Program Owner
Coordinates across all of them

⚠ What can't be delegated to the MSP: policy ownership, affirmation decisions, scope boundaries, and accountability for the program's defensibility.

What governance cadence does a healthy program need?

Monthly
Program review with IT, the MSP, and the program owner

Quarterly
Executive review with the affirming official, legal, and finance

Annually
Full SSP review, SPRS recalculation, and assessment readiness check

On Change
Any new contract, new system, new vendor, or staff turnover in a control-owning role triggers a targeted review

SECTION 7

Cost, Timeline, and ROI

What's the realistic timeline from start to certification?

Most mid-market manufacturers starting from scratch need nine to eighteen months. Companies with established programs that need validation can move faster. Companies that try to compress below nine months usually end up either failing the assessment or paying for rework that erases the time savings.

What are the major phases?

01

Scoping
Define the CUI boundary and what's in and out of scope

02

Gap Assessment
Identify the distance between current state and required state

03

Remediation Planning
Sequence the work, assign ownership, set the budget

04

Technical Remediation
Implement controls, configure tools, segment networks where needed

05

Documentation
SSP, policies, procedures, SRM

06

Evidence Collection
Build the artifact library that proves controls operate

07

Mock Assessment
Pressure-test before formal assessment

08

C3PAO Assessment
The formal certification audit

What stretches the timeline?

- Unclear scope, often from a CUI boundary that wasn't defined first
- Legacy identity systems and unsegmented networks
- Mixed CUI and non-CUI workflows that need to be separated
- OT environments connected to IT environments without segmentation
- Vendor scope that wasn't addressed early
- Documentation that doesn't match operational reality, requiring rewrite or re-implementation

What compresses it?

- A clear, defensible CUI boundary set early
- Existing ITAR or HIPAA discipline that translates
- An MSP that's actually CMMC-aligned, not just CMMC-aware
- Validating while building, instead of remediating after the fact

Why is C3PAO scheduling its own constraint?

There are far more contractors needing assessment than C3PAOs available to assess them. Lead times for formal assessment are months long and growing. Waiting to schedule until you're "ready" usually means waiting again to get on the calendar. Plan the assessment date back from when you actually need certification, not forward from when you finish remediation.

What are the four cost categories executives should weigh?

Cost of Certification
Program build, tools, advisory, and the C3PAO assessment itself

Cost of a Failed Assessment
Rework, re-assessment fees, and the time the company can't bid on new work

Cost of an FCA Action
Legal defense, settlement or judgment, and reputational damage

Cost of Supply Chain Removal
Lost contracts, lost RFQ flow, and lost preferred-supplier status

Where do costs get underestimated?

Documentation. Most companies plan for technical remediation and forget that the SSP, POA&M, evidence library, and SRM take real time to build properly. Internal staff time is the most-missed cost line.

Evidence collection comes second. "We have the controls" and "we can prove the controls operate" are different problems, and the second one is where most assessments fail.

How should we think about CMMC costs in the budget?

Most CMMC costs are allocable to government contracts when properly categorized. Direct costs map to specific contracts; indirect costs flow through overhead or G&A pools. Talk to your finance team and your DCAA-experienced accountant before you start spending. The treatment matters for both pricing and recovery. (Specifics depend on your accounting structure and contract types. This isn't accounting advice.)

How should a CFO compare investment to protected revenue?

Calculate CMMC-touched revenue across all six streams in section 4. Compare it to the all-in cost of certification (build plus assessment plus first-year operations). For most mid-market manufacturers, the protected revenue is one to two orders of magnitude larger than the investment. Frame CMMC as revenue protection, not cybersecurity spend.

Is CMMC a one-time project?

No. Certification is a milestone. Sustained compliance is the program. Recertification cycles, regulatory changes, environmental drift, and ongoing evidence production all require continuous oversight. Build the program with the expectation that you're running it indefinitely, not finishing it.

SECTION 8

Documentation, Evidence, and a Healthy Program

What does "assessment-ready" actually mean?

It means three things, all at once. The controls are implemented and operating. The documentation reflects what's actually happening. The evidence proving both can be produced on demand, in a form an assessor will accept. Most companies fail one of the three, and any one failure is enough to delay or fail certification.

What is a System Security Plan (SSP)?

The master document that describes how your environment implements each NIST SP 800-171 control. It defines scope, ownership, implementation status, and operational reality. It's the gating document for assessment. If the SSP doesn't match what's deployed, the assessment will surface the gap.

Why are "aspirational" SSPs dangerous?

Because they describe what the company wishes were true, not what is true. Assessors test against operational reality, not stated intent. An SSP that's ahead of the implementation is worse than one that's accurate-but-incomplete, because it creates the False Claims exposure described in section 6.

What is a POA&M?

Plan of Action and Milestones. The formal record of controls that aren't fully implemented yet, with timelines and ownership for closing them. CMMC permits POA&Ms for a defined subset of controls, but they must be tracked and closed on schedule. POA&M discipline is one of the things assessors look at hardest.

What's an evidence library?

The organized repository of artifacts that prove each control is operating: configuration screenshots, policy attestations, training records, log samples, ticket histories, change records, vendor agreements. Evidence isn't generated for the assessment. It's generated by the program every day, and collected into the library.

How should evidence be organized?

- By control objective, not by tool or department
- With dates, ownership, and source clearly marked on every artifact
- In a single repository, accessible to the affirming official and reviewable by the assessor
- Refreshed on a defined cadence, with stale evidence flagged automatically

What are the signs of a drifting program?

- The SSP hasn't been updated in more than six months
- The POA&M still lists items from a year ago with no movement
- The affirming official can't answer basic questions about scope or controls
- Evidence has to be hunted down rather than retrieved
- The MSP is the only one who knows how the program is structured
- There's no governance cadence, just reactive responses to customer requests

What should the affirming official be able to answer at any moment?

- What's our current SPRS score, and what changed it last?
- What's our CUI boundary, and what's outside it?
- Which controls are on the POA&M, and when do they close?
- When was the SSP last reviewed, by whom, and against what?
- If a prime asks for our assessment status today, what do we tell them?

SECTION 9

Subcontractors, MSPs, and Shared Responsibility

Are we responsible for subcontractors who handle CUI for us?

Yes. If you flow CUI to a subcontractor, you're responsible for confirming they protect it. Their failures become your findings. This is one of the most-missed exposure areas, especially in finishing, coating, and machining work.

What should we ask downstream vendors?

- Do you handle our CUI, and if so, where does it live in your environment?
- What's your current SPRS score?
- What's your CMMC plan and timeline?
- Will you sign a flow-down agreement that obligates you to protect what we send?
- How do you destroy or return our data when work is complete?

What documentation should subcontractors provide?

At a minimum: a current SPRS score, a written statement of their CMMC posture and timeline, and signed acknowledgment of the flow-down obligations in your contract. For higher-stakes vendors, request their SSP cover page or a third-party validation summary.

How should we maintain an approved supplier list?

Tie inclusion to documented evidence of cyber posture, not just historical relationship. Refresh annually. Vendors who can't or won't provide evidence get flagged for replacement, and the replacement work starts before the contract reason forces it.

What's a shared responsibility matrix (SRM)?

A document that names, for every control in scope, who's responsible: your team, your MSP, an enclave provider, a subcontractor, or some combination. It's the answer to the assessor's question "who does this?" If the SRM isn't clear, control ownership isn't clear, and the program isn't defensible.

What can an MSP own, and what can't they?

MSP CAN own

Technical implementation: identity, endpoint, network, monitoring, patching, backup, and the configuration of tools that support controls. They can also own evidence collection for the technical controls they operate.

MSP CANNOT own

Affirmation, policy decisions, scope boundaries, accountability for the score, or the relationship with the C3PAO. Those stay with the company. An MSP that says "we'll handle CMMC" is either misrepresenting their role or about to take on liability they're not equipped to carry.

Our MSP says we're compliant. Is that enough?

No. The MSP isn't the affirming official, and "compliant" isn't a meaningful claim without evidence of scope, controls, and operational reality. Validate independently. The cost of validation is small. The cost of believing an inaccurate claim and signing on it is large.

SECTION 10

Pre-Assessment and C3PAO Readiness

When should we engage a C3PAO?

When the program is built, the SSP matches reality, the POA&M is current and credible, the evidence library is organized and complete, and a mock assessment has confirmed all of the above. Engaging earlier wastes assessment slots and risks failure.

Why should we run a mock assessment first?

Because formal assessment failure is expensive in time, money, and reputation. A mock assessment finds the gaps that the formal assessment would have found, but with no consequence and no record. For most companies, the mock is the single highest-ROI step in the program.

What does a mock assessment test?

Document Review
Against NIST SP 800-171A objectives

Evidence Production
Can the team produce artifacts on request, in the form an assessor expects?

Interview Readiness
Can control owners describe their controls accurately and consistently?

Scope & Boundary Defensibility
Does the SSP align with the operational environment?

What are common reasons companies fail or delay assessments?

- SSP doesn't match what's actually deployed
- Evidence can't be produced on demand
- CUI boundary wasn't defined defensibly, leaving scope ambiguous
- Control owners can't articulate their own controls under questioning
- MSP-managed controls have unclear shared responsibility
- POA&M items are stale or unrealistic

How should we select a C3PAO?

Sector Experience
Have they assessed manufacturers, especially in firearms or defense supply chain?

Availability
Lead times are long; book early

Methodology
Do they describe a clear process, or does it sound improvised?

Independence
Are they only an assessor, or do they also remediate? Categories that do both create conflicts you don't want

When is delaying assessment by 60 to 90 days the right call?

Whenever a mock assessment surfaces gaps that won't close cleanly in time. Delay costs less than failure. The C3PAO won't grade you on a curve. They'll find what's there, or they'll find what isn't.

SECTION 11

First 90 Days and Practical Next Steps

If we haven't started, what should we do first?

Map where CUI actually lives. Inboxes, laptops, file shares, shop-floor systems, vendor workflows, contract portals, drawing repositories. The map drives every other decision: scope, cost, timeline, vendor, and tooling. Companies that skip this and start with tool selection always pay for it later.

1 2 3

Day 30

- Pull every active and recent contract and search for the DFARS clauses listed in section 3
- Identify the affirming official and brief them on what they're signing for
- Map where CUI lives across the environment, even informally
- Bring legal and finance into the conversation
- Decide who owns the program internally, and who their executive sponsor is

Day 60

- Defensible CUI boundary defined and documented
- Scope statement written and reviewed
- Gap assessment underway against NIST SP 800-171
- Current SPRS score validated, not just inherited
- MSP relationship reviewed against actual CMMC requirements, not marketing claims

Day 90

- Remediation roadmap with sequencing, ownership, and budget
- Governance structure operating: monthly program reviews, quarterly executive reviews
- Initial SSP draft underway
- Subcontractor inventory with CUI flow-down identified
- Realistic timeline to certification, with a target assessment window

What mistakes should we avoid in the first 90 days?

Buying tools before defining scope	Letting the MSP run the program without executive ownership
Treating the SSP as a documentation task instead of an operational document	Affirming a SPRS score without independent review
Assuming "we've been a supplier for 20 years" protects current relationships	Waiting for the next budget cycle before starting any of this

What's the single best first step? Map where CUI actually lives. Then use that map to drive scope, cost, timeline, and risk decisions. Everything else follows from getting that one thing right.

GET STARTED

Get clarity in 60 minutes

The free Fellsway CMMC Readiness Workshop

If you have questions that this FAQ doesn't answer for your specific situation, that's exactly what the workshop is for.

It's a structured, 60-minute consulting session with our CMMC team. Not a sales call. Not a pitch. We work through your environment, your contracts, and your current posture, then give you a single, fact-based recommendation: build a program from the ground up, validate the work you've already done, or move directly to assessment readiness. You leave with clarity, a realistic timeline, and an honest investment range.

It's free. It's fast. And it's the right starting point whether you're at day zero or mid-implementation.

In 60 minutes, you'll know:

- Whether CMMC formally applies to you, and at what level
- Where you actually stand across the four key readiness indicators
- Whether you should validate, build, or move to assessment
- What your realistic timeline and investment range looks like
- Exactly what to do next

Schedule your free CMMC Readiness Workshop

fellsway

Risk is constant.

Ready is a choice.

BE COMPLIANT · BE RESILIENT · BE READY

Are you ready? Talk to us

fellswaygroup.com

APPENDIX

Glossary

CMMC
Cybersecurity Maturity Model Certification. The DoD framework governing cybersecurity for defense contractors.

FCI
Federal Contract Information. Information generated for or under federal contract that isn't intended for public release.

CUI
Controlled Unclassified Information. Sensitive federal information requiring protection under specific safeguards.

DFARS
Defense Federal Acquisition Regulation Supplement. The regulation that flows cybersecurity requirements into DoD contracts.

NIST SP 800-171
The NIST publication defining the 110 security controls required to protect CUI in non-federal systems.

SPRS
Supplier Performance Risk System. The DoD portal where contractors post their NIST SP 800-171 self-assessment scores.

SSP
System Security Plan. The master document describing how your environment implements each required control.

POA&M
Plan of Action and Milestones. The formal record of controls not yet fully implemented, with closure timelines.

C3PAO
CMMC Third-Party Assessment Organization. The accredited bodies that perform formal CMMC Level 2 assessments.

Affirming Official
The executive who signs to confirm the accuracy of a contractor's SPRS score and cybersecurity representations.

FCA
False Claims Act. The federal statute that creates liability for false representations made to win or hold federal contracts.

Qui Tam
A whistleblower action filed under the FCA on behalf of the government, with the whistleblower entitled to a portion of recovery.

Flow-Down Clause
A contractual provision passing obligations from a prime to its suppliers, and from those suppliers to theirs.

Shared Responsibility Matrix (SRM)
A document specifying which party (you, MSP, enclave, vendor) owns each control in scope.

CUI Boundary
The defined perimeter within which CUI is permitted to flow, store, and be processed.

FMS
Foreign Military Sales. US government program for selling defense articles to allied nations.

ITAR
International Traffic in Arms Regulations. The US export control regime governing defense articles and technical data.