

THE DEFENSE RAMP-UP IS HERE:

A Sub-Tier Manufacturer's
Guide to Operational and
Compliance Readiness



EXECUTIVE SUMMARY

The Department of Defense (DOD)¹ is bypassing traditional Tier 1 primes and pulling sub-tier manufacturers into the munitions and weapons supply chain faster than most are prepared for. Firms at Tier 2, Tier 3, Tier 4, and below face operational and compliance expectations that most aren't currently equipped to meet.

Global conflicts are burning through munitions at historic rates, defense budgets are expanding, and policy is explicitly pushing prime contractors to broaden the defense industrial base (DIB). The U.S. government has framed the "factory floor" as strategically significant, which means your shop floor matters in ways it didn't five years ago.

The risk is scaling into defense programs without the manufacturing execution discipline and system controls that primes and auditors will demand from day one. Defense contracts require documented traceability from every shop-floor event through inventory, labor, and cost reporting. They require enterprise resource planning (ERP) systems configured for government cost allocation and accounting structures that satisfy Defense Contract Audit Agency (DCAA) scrutiny, along with quality and production controls subject to Defense Contract Management Agency (DCMA) oversight on the shop floor.

They also require a cybersecurity posture certified under the Cybersecurity Maturity Model Certification (CMMC) program before contract award. Gaps in any of these areas can trigger payment withholding or False Claims Act (FCA) exposure, and in some cases, disqualification from award entirely.

The gaps are fixable but correcting them takes time. Configuring ERP systems for government cost allocation, building compliant accounting and timekeeping structures, and achieving cybersecurity certification can take 6 to 12 months, and that work is far more expensive when it's happening mid-contract under audit pressure.

What ties these requirements together is a single operating concept: defense readiness. This is the ability to produce audit-ready evidence automatically from the system of record — ERP, timekeeping, inventory, and quality — as a byproduct of daily operations rather than as a separate reporting exercise. Each specific requirement is a particular application of that principle, and the manufacturers who internalize it close the gap on their terms rather than the government's.

This report outlines what defense readiness requires, the costs of falling behind, and how to close the gap before the contract arrives.

¹ Executive Order 14347, *Restoring the United States Department of War*, 90 FR 43893 (Sept. 10, 2025), authorized "Department of War (DOW)" as a secondary title for the Department of Defense in official correspondence, public communications, and non-statutory documents. The "Department of Defense (DOD)" remains the legal entity under Title 10 U.S.C. This report uses DOD throughout the body for consistency with the statutory and regulatory authorities cited (DFARS, FAR, DCAA, DCMA, etc.); citations retain the "Department of War (DOW)" branding where source documents were published under that title.

Key Takeaways

- + The DOD is actively bypassing traditional Tier 1 primes by awarding direct prime contracts to non-traditional small- and mid-sized (SMB) manufacturers, while simultaneously deepening visibility and scrutiny into sub-tier supply chains.
- + Defense readiness requires producing consistent, high-volume output with full traceability across shop-floor activity, inventory, labor, and cost reporting.
- + Defense readiness means generating audit-ready evidence automatically from your system of record, rather than reconstructing it per audit. It's the concept behind DCAA, DCMA, and DFARS business system compliance, including MMAS.
- + While the readiness gap is fixable, closing it takes months of configuring production, ERP, and cybersecurity controls to meet defense requirements before audit.
- + Stockpile drawdowns across Ukraine, Israel, and the Iran campaign have created sustained munitions demand that will persist regardless of how conflicts resolve.
- + Lack of readiness creates immediate cash-flow risk, as disapproved business systems trigger payment withholding and DCAA is both incentivized and equipped to identify deficiencies.
- + Manufacturing readiness is a competitive advantage in federal contracting, and CTND's free business review helps manufacturers build a roadmap to achieve compliance.



KEY TAKEAWAYS

- The DOD is actively bypassing traditional Tier 1 primes by awarding direct prime contracts to non-traditional small- and mid-sized (SMB) manufacturers, while simultaneously deepening visibility and scrutiny into sub-tier supply chains.
- Stockpile drawdowns across Ukraine, Israel, and the Iran campaign have locked in a munitions replenishment demand signal that won't slow regardless of how current conflicts resolve. Army 155mm shell production still falls roughly 44,000 rounds per month short of target.
- Defense readiness is the ability to produce audit-ready evidence automatically from the system of record — ERP, timekeeping, inventory, and quality — rather than reconstructing it for each audit. This is the organizing concept behind DCAA, DCMA, and Defense Federal Acquisition Regulation Supplement (DFARS) business system compliance, and it's what the Material Management and Accounting System (MMAS) and accounting system requirements under DFARS formalize and the government actively audits.
- Being unready has direct cash-flow consequences. A disapproved business system triggers payment withholding, and DCAA has the financial incentive and resources to find deficiencies.
- The readiness gap is fixable, but closing it takes months. Production scheduling, quality and traceability systems, and ERP, accounting, and cybersecurity controls must be configured to meet defense requirements before the first audit.
- Readiness is a competitive advantage. Federal acquisition rules make manufacturing readiness a scored evaluation criterion in source selections, and primes select sub-tier suppliers on the same basis.
- Cre8tive Technology and Design's (CTND) free business review identifies specific gaps between your current systems and defense requirements, and delivers a roadmap with timeframes and cost estimates for closing them.

WHAT'S DRIVING THE SURGE IN DEFENSE EQUIPMENT DEMAND AND MANUFACTURING

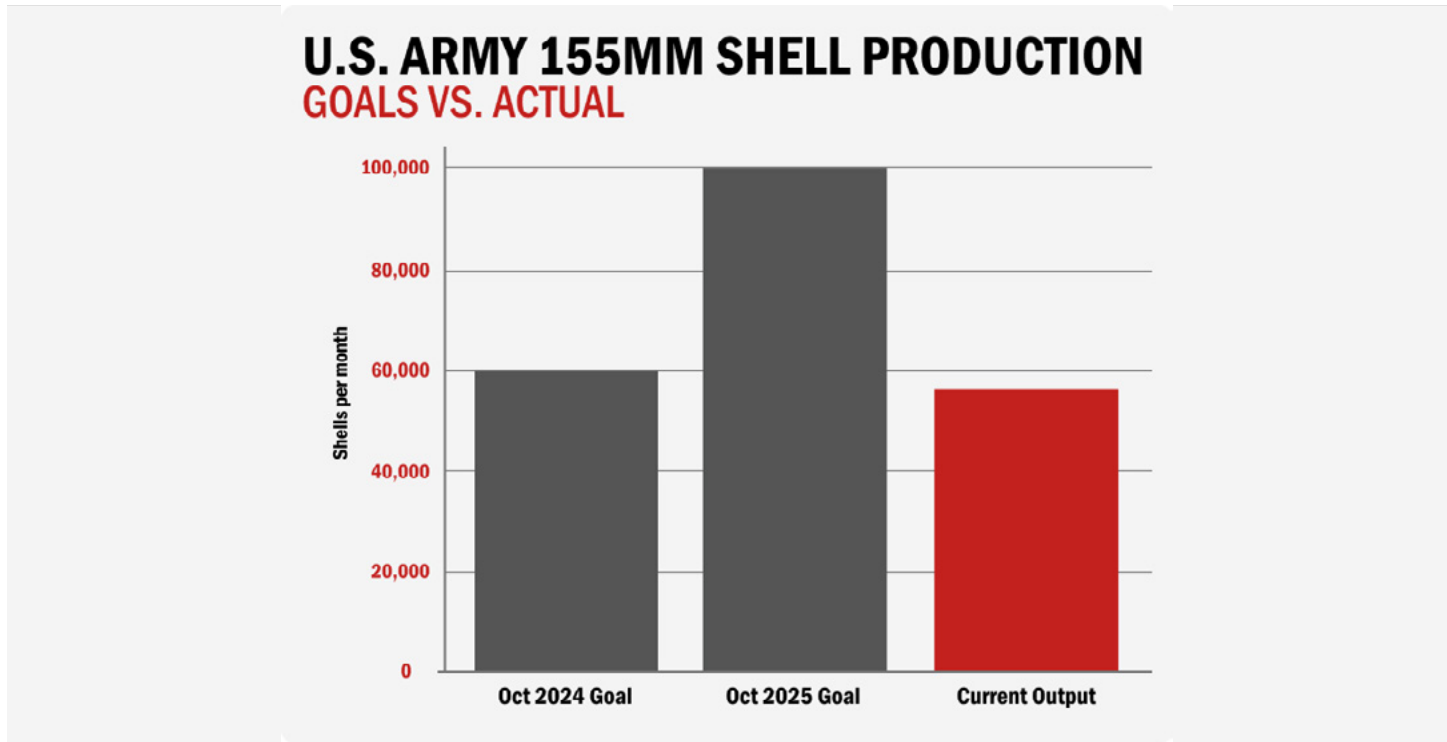
The U.S. government is restructuring its entire defense acquisition architecture around the operational reality that it can't produce munitions and weapons fast enough to meet the demands of the current threat environment. Here's why.

Stockpile Drawdowns and Production Shortfalls

Russia’s invasion of Ukraine triggered a sustained drawdown of U.S. munitions stockpiles that the Army has spent years scrambling to replenish. In March 2025, the State Department said the U.S. had sent more than 3 million 155mm shells to support Ukraine since the invasion started. At that point, the U.S. had also delivered tens of thousands of rounds to Israel following its 2023 conflict with Hamas.^[1]

Then came Iran. In just the first 72 hours of Operation Epic Fury, which U.S. Central Command (CENTCOM) described as “the largest regional concentration of American military firepower in a generation,” the U.S. expended an estimated 400 cruise missiles, representing roughly 10 percent of total inventory, and approximately 100 antiballistic missiles.^{[2][3]}

Depleted stockpiles are only half the problem. The Army’s 155mm shell production numbers show just how difficult it’s been to rebuild capacity. In early 2024, the Army set a goal to reach 60,000 shells per month by October 2024 and 100,000 per month by October 2025.^[4] Two years later, output stands at approximately 56,000 per month, still short of both targets.^[5]



Decades of post-Cold War consolidation created these conditions. The DIB contracted from 51 prime vendors after the Cold War down to just five major prime contractors today, which build sophisticated systems at low volume over long timelines. That structure was never designed for the rapid, high-volume production surge the current threat environment demands.

Consider the lag at an Army facility in Mesquite, Texas. The Army contracted General Dynamics Ordnance and Tactical Systems (GD-OTS) to stand up three 155mm shell production lines in 2024. Two years later, the facility *has yet to produce a single projectile*.^[5] The Army has attempted to compensate for the ongoing shortfall. In September 2025, it awarded Global Military Products, based in Tampa, FL, a \$639 million contract to produce 155mm shells as part of a broader push to bring new manufacturing capacity online.^[1] Yet almost halfway through 2026, the DIB is still roughly 44,000 shells behind per month.

Strategic Threat Response and Structural Failures

The 2026 National Defense Strategy puts the risk in plain terms. The U.S. faces a credible possibility of being drawn into simultaneous major wars across theaters, and this scenario exposes the full weight of decades of underinvestment in domestic DIB manufacturing capacity.^[6]

A May 2025 presidential determination invoked the Defense Production Act (DPA), finding that action was necessary to increase production capacity of munitions, missiles, and associated equipment, and that shortfalls would severely impair national defense capability.^[7] Presidents reserve DPA invocations for moments when the standard acquisition process can't move fast enough to address a national security gap.

The November 2025 Warfighting Acquisition System memo named the structural failures responsible for the gap: The acquisition system suffers from fragmented accountability, in which no single leader has the necessary authority to lead programs and deliver results urgently. It also has broken incentives that reward fully satisfying every requirement and specification at the expense of on-time delivery, and constrained industrial capacity that can't surge or adapt quickly.^[8]

The consequences are measurable. The Government Accountability Office (GAO) reported in June 2025 that the expected time frame for major defense acquisition programs to provide warfighters with even an initial capability



is now *almost 12 years from program start*.^[9] The memo's remedy is to put the entire acquisition system and DIB on a wartime footing, with urgency and a mandate to accept more risk.

The Iran Campaign and Its Procurement Impact

The Iran campaign converted policy urgency into a procurement emergency. Operation Epic Fury launched on February 28, 2026, and by March 3, the Trump administration had convened chief executives from the country's largest defense contractors at the White House, pressing them to accelerate output as the Pentagon moved to replenish supplies drawn down across multiple conflicts.^[10]

According to a closed-door Pentagon briefing to Senate appropriators reported by NBC News on March 12, the first six days of the conflict cost more than \$11.3 billion.^[11] The conflict consumed longer-range missiles not previously furnished to Ukraine or Israel, opening new categories of shortfall on top of existing ones.^[10]

The scale of stockpile replenishment needs grew rapidly as operations continued, and by March 19, Defense Secretary Pete Hegseth confirmed the Pentagon planned to ask Congress for approximately \$200 billion in supplemental funds to pay for Iran operations and refill munitions stockpiles.^[12] By early April, the administration was expected to scale back the request to between \$80 billion and \$100 billion, but the supplemental funding request hadn't yet been formally submitted to Congress.^{[13][14]}

A two-week ceasefire brokered by Pakistan took effect on April 8, but talks in Islamabad collapsed on April 12 without agreement, and the U.S. subsequently announced a naval blockade of Iranian ports.^[15] The conflict's trajectory remains uncertain, but the demand signal for munitions replenishment is already locked in regardless of the outcome.

Policy and Funding Responses

Washington formalized its response before Iran accelerated the timeline. An April 2025 executive order called for a comprehensive overhaul of the Defense Acquisition System (DAS), now coined the Warfighting Acquisition System (WAS), with an explicit emphasis on speed, execution, and cutting through red tape. The order's goal was to accelerate U.S. defense procurement and revitalize the DIB, because "the factory floor can be just as significant as the battlefield."^[16] The DOW's Acquisition Transformation Strategy followed in November 2025, issuing operational directives to prioritize schedule and volume to deliver manufacturing capability sooner and to encourage more innovative American companies to build military equipment.^[17]

Congress moved on the funding side in parallel. On February 3, 2026, the President signed the "Consolidated Appropriations Act, 2026" into law.^[18] The numbers signal a government that has accepted the production gap as a permanent structural problem: \$3 billion for munitions production and research and development, \$650 million to expand solid rocket motor production capacity, \$500 million for PATRIOT PAC-3 missiles, and \$6.3 billion for shipbuilding, bringing total naval procurement in the bill to \$27.2 billion.^[19]

What This Means for the Supply Chain

In practice, this means pushing existing primes to produce faster and bypassing traditional Tier 1 primes to award direct prime contracts to non-traditional SMB manufacturers. This helps deliver the volume and variety that five primes alone can't handle, while deepening visibility and scrutiny into sub-tier supply chains.

"The turbulence in the global economy is translating directly into demand for weapon systems and component replacement at a scale most manufacturers haven't planned for," says Bob Aronson, Chief Revenue Officer at Cre8tive Technology and Design. "The companies we see succeeding are the ones that treat technology as a manufacturing accelerator."



**"The companies we see succeeding
are the ones that treat technology as
a manufacturing accelerator."**

BOB ARONSON

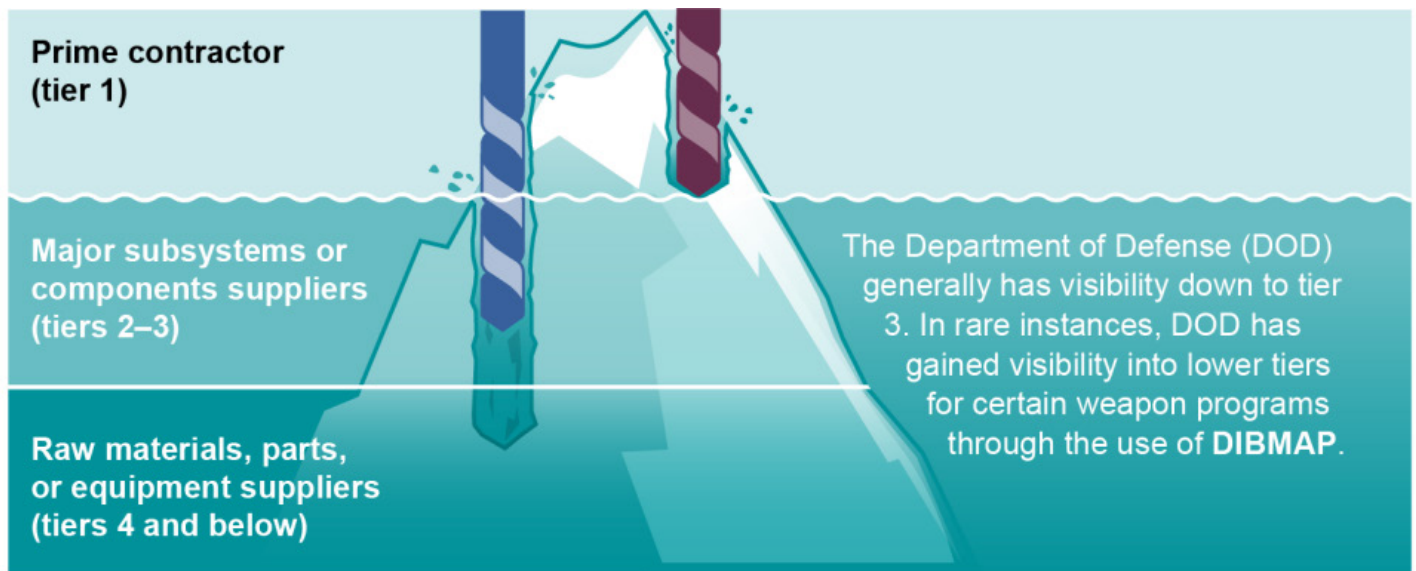
Chief Revenue Officer, Cre8tive Technology and Design

The National Defense Strategy frames the DIB challenge as a replenishment exercise and a once-in-a-century revival of American industry. The strategy has an explicit goal of returning the U.S. to the status of the "world's premier arsenal," one that can produce for ourselves and our allies and partners at scale, rapidly, and at the highest quality levels.^[6] Achieving that goal requires depth across the entire supply chain, well beyond the prime level. The WAS makes this explicit, calling for expanding manufacturing capacity in the national DIB to prepare for surge production if deterrence fails.^[20]

But a March 2026 Reagan Institute report found that while public and private capital are scaling production across the defense industrial base, structural fragilities remain in sub-tier supply chains.^[21] The ambition and the infrastructure haven't caught up to each other yet.

ALL EYES ON MID- AND LOW-TIER DEFENSE MANUFACTURERS

The DIB relies on a global network of more than 200,000 suppliers to produce weapon systems and noncombat goods across multiple tiers, from major subcontractors down through the sub-tier suppliers of parts, components, and raw materials that form the hidden foundation of everything primes deliver. The DOD generally has visibility down to Tier 3.^[22] Below that, the supply chain becomes largely opaque, and that's precisely where much of the government's expansion effort is now pointed. When the government pushes for more volume and faster delivery, that pressure moves down the chain.



Source: [GAO-25-107283, Defense Industrial Base: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers, July 2025.](#)

“The DOD is now issuing contracts directly to sub-tier suppliers that would have gone exclusively to the large primes a few years ago. That’s a real opportunity,” says Aronson. “But these suppliers are also being asked to design, develop, and produce defense-ready solutions while maintaining full compliance with requirements they may never have encountered in commercial work.”

The recognition of this reality is clear in government policy and testimony. In June 2025, the Acting Assistant Secretary of Defense for Sustainment, Steven J. Morani, told the House Armed Services Subcommittee on Tactical Air and Land Forces that DIB improvements throughout several cross-cutting, sub-tier suppliers ensure continued support for operational plans beyond initial inventory levels. The Department was actively targeting critical new domestic suppliers to expedite qualification, scale-up, and to adopt new technology across munitions, components, and long-lead items.^[23]

THE DEFENSE RAMP-UP IS HERE:

The Defense Business Board (DBB) put it in starker terms in its 2024 Industry Partnerships for Crises study. The study proposed immediate actions the DOD could take to establish, structure, and manage relationships with the private sector to quickly expand capacity across a broad array of products. To do so, the DOD must rethink its own policies, adopt novel contracting approaches, possibly pursue statutory changes, enter into new partnership agreements, and make additional investments in the domestic DIB in ways it hasn't before.^[24]

The DOD is now issuing contracts directly to sub-tier suppliers...That's a real opportunity. But these suppliers are also being asked to produce defense-ready solutions...with requirements they may never have encountered in commercial work.

BOB ARONSON
Chief Revenue Officer
Cre8tive Technology and Design



Congress has spent two legislative cycles actively lowering the cost of entry for smaller manufacturers: The FY25 National Defense Authorization Act (NDAA) reduced barriers to subcontract pricing requirements and launched pilot programs designed to bring nontraditional contractors and small businesses into defense work.^[25]

A pending Senate bill, the FY26 NDAA, goes further. If enacted, it would prohibit the government from flowing certain [defense compliance](#) requirements down to subcontractors supplying commercial products, removing a category of regulatory burden that has historically priced smaller manufacturers out of defense contracts. It would also create new exemptions from DFARS requirements for nontraditional defense contractors and require prime contractors to actively expand their supply sources at every tier of the supply chain. The APEX Accelerators program (formerly Procurement Technical Assistance Centers), updated under the bill, would carry an explicit mandate to diversify and expand the DIB.^[26]

The invitation comes with expectations attached. As the government broadens its supplier base, it's simultaneously increasing its visibility into and scrutiny of the lower tiers. The DOD has yet to identify resources, priorities, and time frames for completing the integration of supply chain visibility efforts, and hasn't identified the organization responsible for implementing leading commercial practices for identifying foreign dependency risks.

^[22] But it's actively building the tools and contractual mechanisms to see deeper into the supply chain, and sub-tiers that aren't operationally ready when that scrutiny arrives will face consequences that extend well beyond a single contract.

WHAT MANUFACTURING READINESS MEANS FOR DEFENSE INDUSTRIAL GROWTH

Defense work generates an evidence requirement that commercial work doesn't. When a government auditor asks how a specific lot of material moved from receiving through production into a billed deliverable, or how a specific labor hour was assigned to a specific contract, the answer must come from documentation that already exists. That requirement runs through every business system the government evaluates, every regulation contractors are measured against, and every audit they will face during contract performance.

This is the organizing concept behind defense readiness.

“Defense Readiness is the ability to produce audit-ready evidence automatically from the system of record — ERP, timekeeping, inventory, and quality — as a byproduct of daily operations rather than as a separate reporting exercise.”

It is the single most important concept in DCAA, DCMA, and DFARS business system compliance. Every requirement these authorities test, such as MMAS accuracy thresholds, labor charging discipline, cost segregation, material traceability, and supplier qualification, ultimately comes down to whether the system of record can answer the auditor's questions without manual intervention.

A manufacturer that internalizes this principle and configures systems accordingly will satisfy each individual requirement as a matter of course. One that treats compliance as a series of separate reporting obligations will find each one expensive to satisfy and difficult to defend under audit pressure.

DEFENSE MANUFACTURING READINESS

PRE-AWARD SURVEY (SF 1408) + Tests cost segregation and GL control + Required before cost-reimbursement award (FAR 16.104) + Gap here blocks the contract itself	PRODUCTION EXECUTION + Contract-driven scheduling and delivery + Consistent and scalable output + Alignment to program timelines	TRACEABILITY & DOCUMENTATION + End-to-end visibility across materials, labor, and processes + As-built records tied to every deliverable + Audit-ready at any point in production	MATERIAL MANAGEMENT (MMAS) 98% BOM accuracy 95% Schedule accuracy 95% Inventory accuracy	COMPLIANT ACCOUNTING + Labor charged at the point of entry to defined cost objectives + Clear segregation of direct versus indirect costs + DFARS-compliant financial and cost reporting
---	---	--	--	---

ERP + SCHEDULING SYSTEMS

Integrated systems that connect production, inventory, labor, and cost—ensuring traceability is maintained and compliance evidence is generated automatically.

Readiness begins on the production floor, but it doesn't stay there. Primes must prioritize schedule and volume to deliver capability sooner. That directive applies to every supplier in the chain, which will feel pressure to move faster, produce more, and prove, at any point in the program, exactly how they built what they built.

The proof requirement lives in two main places in the regulatory framework:

1. MMAS: Under DFARS 252.242-7004, an MMAS is a contractor's system for planning, controlling, and accounting for the acquisition, use, issuing, and disposition of material. It's the infrastructure that connects your material requirements planning, inventory, and contract cost reporting. The clause sets measurable targets of:

- 98 percent for bill-of-materials accuracy
- 95 percent for master production schedule accuracy
- 95 percent for physical inventory record accuracy.^[27]

If a government auditor asks how a specific lot of material moved from receiving through production to a billed deliverable, your MMAS must provide documentation to support that answer.

2. Accounting System Requirements: Under DFARS 252.242-7006, a compliant accounting system gathers, records, classifies, and presents accurate financial data for government reporting, with subsystems covering billing, labor, indirect costs, and compensation.

For manufacturers used to commercial accounting practices, the most common gap is labor charging.

The clause requires:

- A timekeeping system that identifies each employee's labor by intermediate or final cost objective
- A labor distribution system that charges direct and indirect labor to the appropriate cost objectives
- An auditable chain from source data to billed cost, which means any spreadsheet between the system of record and a government invoice must be controlled and traceable

A timekeeping system that doesn't enforce that discipline at the point of entry is a liability the moment the DCAA arrives. When an auditor identifies material weaknesses, the contractor has 30 days to respond and 45 days after final determination to correct them or submit an acceptable corrective action plan. A disapproved accounting system can trigger payment withholding under DFARS 252.242-7005.^{[28][29]}

For many sub-tier manufacturers, the first formal encounter with these requirements comes before contract award. Under FAR 16.104, the government can't award a cost-reimbursement contract unless the contractor's accounting system is determined adequate for accumulating costs.^[30] DCAA conducts that determination using Standard Form 1408 (SF 1408) as a pre-award survey, testing whether the system segregates direct and indirect costs, identifies costs by contract, accumulates costs under general ledger control, and supports the timekeeping and labor distribution requirements of DFARS 252.242-7006.^{[31][28]}

A system that doesn't meet SF 1408 criteria prevents the contract from being awarded. SF 1408 adequacy is binary. Systems are either adequate or not. The remediation timeline is the same 6 to 12 months either way, but the cost of discovering the gap during a pre-award survey is the contract itself.

THE COST OF BEING BEHIND: WHERE READINESS BREAKS (AND WHAT IT COSTS)

Pre-award is the first gate. Once a manufacturer clears it, the same systems that were evaluated on paper must produce evidence in practice — and that's where most failures surface.

A failure rarely announces itself with an audit finding. It shows up first as operational pressure, like orders falling behind schedule, material costs that can't be traced to a specific contract, or labor hours that don't reconcile with what was billed. By the time a government auditor arrives, the chaos on the shop floor has already become chaos in the books. The audit finding is just the moment it becomes official.

The Cash-Flow Cost of a Disapproved System

Under DFARS 252.242-7005, a business system disapproval on a covered contract triggers a 5 percent payment withholding for deficiencies in any single business system, rising to a maximum of 10 percent if deficiencies are found across multiple systems simultaneously. The clause covers six business systems: accounting, earned value management, estimating, material management and accounting, property management, and purchasing. A manufacturer that submits an acceptable corrective action plan within 45 days and actively implements it can reduce the withholding to 2 percent while remediation is underway.^[29]

Withholding doesn't apply to fixed-price line items where performance is complete and the government has accepted delivery, so the cash-flow risk scales with contract type. On a cost-reimbursement or time-and-materials contract, the exposure is real. At 5 percent withholding on a \$5 million contract before a corrective action plan is accepted, that's \$250,000 in inaccessible cash. At 2 percent during active remediation, it's \$100,000. On a \$10 million contract, those numbers double. The math is straightforward, but the timing isn't always in the manufacturer's control. CTND typically works with clients for 6 to 12 months to bring systems into compliance, and that's the window during which those dollars stay locked up.

THE SCALE OF DCAA OVERSIGHT

The scale of DCAA oversight increases the likelihood of discovering business system deficiencies and cost misallocations. In FY 2025, DCAA examined \$788.4 billion in contract costs, issued 2,480 audit reports and 7,047 memos, and identified \$5.3 billion in savings, realizing a return on investment of \$7.60 per dollar spent.^[32] DCAA has a direct financial incentive to find deficiencies and the resources to do it.

Cybersecurity: A Separate Category of Risk

Cybersecurity failures carry a distinct risk category. The Department of Justice's (DOJ) Civil Cyber-Fraud Initiative has produced a steady stream of FCA settlements against defense contractors who failed to meet DFARS cybersecurity requirements.

"When auditors find deficiencies, the government can and does terminate contracts," says Aronson. "We've seen it happen to publicly traded companies with established defense programs. We've also seen clients go from a \$1 million contract to a \$5 million contract almost overnight when a competitor loses their standing, and the opportunity moves down the list."

When auditors find deficiencies, the government can and does terminate contracts...We've also seen clients go from a \$1 million contract to a \$5 million contract almost overnight when a competitor loses their standing.

BOB ARONSON

Chief Revenue Officer, Cre8tive Technology and Design

In April 2025, the DOJ announced an \$8.4 million settlement resolving allegations that Raytheon violated the FCA by falsely representing compliance with federal cybersecurity regulations.^[33] In July 2025, a California defense contractor and its private equity firm agreed to pay \$1.75 million to resolve FCA liability for knowingly failing to comply with cybersecurity requirements in a Department of the Air Force contract.^[34] These aren't outliers. DOJ's Civil Cyber-Fraud Initiative drove multiple settlements in 2025 involving defense contractors, signaling that cybersecurity compliance remains a priority enforcement area for companies doing business with the government.^[35]

The cybersecurity compliance environment is also tightening, removing the self-reporting flexibility many sub-tier manufacturers have relied on. Until recently, cybersecurity compliance under DFARS was largely self-certified. The CMMC program's final rule, effective November 10, 2025, changes that for contractors handling Controlled Unclassified Information (CUI), which is sensitive government data that isn't classified but must be protected under law. Under CMMC Level 2, third-party assessors certified by the DOD and independent of the contractor

verify compliance directly. There's no approximation and no self-reporting.^[36] A manufacturer that handles CUI and can't pass a third-party assessment faces disqualification.

DFARS CYBERSECURITY REQUIREMENTS AT A GLANCE

DFARS CYBERSECURITY FOUNDATIONS

- + NIST SP 800-171 controls (110 required)
- + Protection of CUI
(Controlled Unclassified Information)
- + Documented policies, access controls,
and system security plans
- + Ongoing monitoring and incident response

VALIDATION SHIFT: CMMC LEVEL 2 ENFORCEMENT

- + No more self-certification
- + Mandatory third-party assessment (C3PAO)
- + Certification required before contract award
- + Applies to contractors handling CUI

ENFORCEMENT & RISK

- + FCA liability for false compliance claims
- + Disqualification from contract award
- + Multi-million-dollar settlements
- + Increased audit scrutiny across suppliers

CTND has seen both sides of this dynamic. Most clients arrive already in some form of audit or compliance review, which is what drives the technology decision. The manufacturers who move proactively close the gap on their terms. The ones who wait close it on the government's terms.

THE SUBCONTRACTOR'S READINESS PLAYBOOK: MANUFACTURING EXECUTION PLUS COMPLIANCE- GRADE SYSTEMS

Readiness is an operating cadence that runs continuously and generates compliance evidence as a byproduct of daily work. The goal is to run an operation where an audit finds nothing surprising.

That cadence has three components, each building on the previous: stabilizing production control and scheduling, tightening quality and traceability, and configuring ERP, accounting, and cybersecurity controls for defense work.

Stabilize Production Control and Scheduling

Defense contracts aren't commercial orders. Delivery schedules carry contractual weight, and the labor and material records tied to those schedules become the evidence base for every billing and audit interaction that follows.

"The shift from commercial scheduling to defense delivery expectations is bigger than most manufacturers anticipate," says Aronson. "In commercial work, a schedule slip is a customer service issue. In defense work, it's a contract performance issue that generates documentation requirements."

A manufacturer moving from commercial work into defense needs to treat scheduling as a compliance function.

In practice, that means a
resource-planning system that:

- Allocates materials, labor, and machine time to specific contracts
- Tracks progress against the master production schedule in real time
- Generates documentation at each stage



Smart scheduling and resource planning sit at the intersection of these requirements. A manufacturer that can't plan and execute production against a contract schedule can't generate the labor and material records the government needs to validate costs. When a supplier delay forces a schedule change, a properly configured [defense ERP system](#) reorders tasks and preserves the traceability chain rather than breaking it. When a government auditor asks why a specific lot of material moved the way it did, the answer must be in the system. Scheduling discipline is a planning and compliance function in defense work, and the system supporting it must be built accordingly. CTND's [aerospace scheduling and resource planning framework](#) addresses exactly this operating challenge.

Tighten Quality and Traceability

Defense work requires documented, defensible traceability from receipt of raw materials through final delivery. The compliance disciplines below are the foundation of what a manufacturer does day to day to build the evidence base that DCMA inspections and DCAA audits will measure against. The foundation is a consistent set of [general manufacturing practices \(GMPs\)](#): documented procedures, qualified personnel, process monitoring, validated workflows, and a culture of continuous improvement applied to every stage of the production lifecycle.

For manufacturers already running lean practices like 5S (Sort, Set in order, Shine, Standardize, Sustain) on the shop floor, that discipline is a direct on-ramp to the documentation and orderliness defense work requires.

“Sub-tier manufacturers entering defense work quickly discover that compliance runs deeper than they expected,” says Aronson. “Export controls, genealogy tracking, as-built records, certificates of compliance, first-article inspection, and flight-worthiness tags aren’t edge cases.”

DEFENSE QUALITY & TRACEABILITY REQUIREMENTS FOR SUB-TIER CONTRACTORS



The compliance requirements that most commonly surface as gaps for sub-tier manufacturers entering defense work include:

- **Contract flow-down:** Mandatory FAR and DFARS clauses that prime contractors must flow down to subcontractors at all tiers, including quality clauses, cybersecurity requirements, and export controls.^{[37][38]}
- **Defense Priorities and Allocations System (DPAS)-rated order prioritization:** Under 15 CFR Part 700, the DPAS assigns priority ratings (DO and DX) to defense contracts and any subcontracts or purchase orders supporting them. A manufacturer that receives a rated order is legally required to accept it and schedule it ahead of unrated commercial work, and under § 700.13(b)(1), scheduling conflicts with previously accepted commercial orders are explicitly not sufficient grounds for rejection. DX-rated orders take precedence over DO-rated orders, and both take precedence over unrated work. The rating travels with the order through every tier of the supply chain, which means a sub-tier manufacturer can receive a rated order from a customer they didn't know was working on defense and must flow that rating down to their own suppliers. For a shop with established commercial customers, the effect is that defense work can displace existing production commitments at any point in the contract. The obligation is to the rating, not to the order of receipt. Rejection requires written notification within 15 working days for DO orders and 10 for DX, and is permitted only under the narrow grounds defined in § 700.13(c), such as the customer's inability to meet established payment terms or the order falling outside the supplier's normal product line. A rating is not required on orders under \$125,000 (or half the Simplified Acquisition Threshold, whichever is greater) if timely delivery can be obtained without it.^[39]
- **First article inspection:** A documented verification process under FAR 52.209-3 confirming the first production unit meets all contract requirements before full production begins. The government may approve, conditionally approve, or disapprove the first article, and production can't proceed without that determination.^[40]
- **As-built records:** Traceable documentation of exactly how each unit was built, including materials incorporated, labor performed, and any deviations from specification. This is typically required through quality clauses and contract data requirements incorporated into individual defense contracts.
- **Certificates of conformance (COC):** Formal written attestation that delivered items meet all specified contract requirements. Under FAR 46.315, a COC may be used at the contracting officer's discretion as a substitute for source inspection when acceptance on that basis is in the government's interest.^[41] In practice, COC requirements are commonly incorporated into defense contracts through contract data requirements and quality clauses.
- **Approved supplier management:** Documented processes for selecting and qualifying suppliers that meet contract quality requirements. Under DFARS 252.244-7001, contractors are required to procure from responsible and reliable sources and ensure those sources meet applicable quality requirements.^[38] For contractors with qualifying DOD sales exceeding \$25 million, this is enforced through the DCMA Contractor Purchasing System Review (CPSR) process.^[42] For sub-tier manufacturers below that threshold, the obligation flows through prime contractor flow-down clauses under 252.244-7001(c)(19), which require primes to flow purchasing system and quality requirements down through the supply chain.^[38]

- **Prohibited Party & Debarment Screening (commonly called Denied Party Screening in industry practice):**

Systematic screening of all suppliers, vendors, and key personnel against the System for Award Management (SAM) Exclusions list, which consolidates parties suspended, debarred, proposed for debarment, voluntarily excluded, or otherwise declared ineligible for federal awards. Under FAR Subpart 9.4, contractors are prohibited from entering subcontracts in excess of \$45,000 (other than for commercially available off-the-shelf items) with any party listed in SAM Exclusions unless the agency head determines in writing that there is a compelling reason. Under DFARS 252.209-7004, contractors are also prohibited from subcontracting with entities owned or controlled by the government of a country designated as a state sponsor of terrorism, unless the Secretary of Defense waives this prohibition. Screening is a mandatory ongoing obligation, not a one-time check at onboarding. The SAM Exclusions list is updated continuously, and a supplier that was clean at contract start can become excluded mid-performance.^{[43][44]}

- **Flight worthiness tags:** Documented verification that components going into airborne systems meet airworthiness standards and have been processed through an approved quality chain. This requirement is embedded in A&D contract quality clauses and is a core feature of the [CTND A&D compliance solution](#).
- **Export controls:** Regulatory controls governing the export of defense articles, services, and technical data. International Traffic in Arms Regulations (ITAR), administered by the State Department's Directorate of Defense Trade Controls, covers items on the U.S. Munitions List (USML).^[45] Export Administration Regulations (EAR), administered by the Commerce Department's Bureau of Industry and Security (BIS), governs dual-use items on the Commerce Control List (CCL).^[46] Sub-tier manufacturers producing components for weapons systems, aircraft, or other controlled platforms are almost certainly handling ITAR- or EAR-controlled technical data and must register, correctly classify their products, and control access accordingly.

A manufacturer that hasn't built these disciplines into daily operations will find it nearly impossible to retrofit under the time pressure of a defense contract. The documentation gap that looks manageable during the bid and proposal becomes a material weakness finding six months into performance.

The disciplines above are what a manufacturer does to generate audit-ready evidence as a byproduct of daily operations. Two authorities then measure that evidence against contractual requirements: DCMA on the shop floor through quality assurance and surveillance, and DCAA through the formal business system audits covered below. DCMA is the authority a sub-tier manufacturer is most likely to meet first.

DCMA OVERSIGHT: THE AUTHORITY ON THE SHOP FLOOR

Under FAR Part 42, DCMA is responsible for 71 contract administration functions on behalf of contracting agencies, including production surveillance, quality assurance, and contractor business system reviews.^[47]

For sub-tier manufacturers, five DCMA touchpoints matter most:

1. Source Inspection: Under FAR 46.402 and DFARS

246.103, the government may require quality assurance and acceptance at the contractor's facility before delivery rather than after.^{[48][49]} When a contract specifies source inspection, a DCMA Quality Assurance Representative (QAR) physically verifies that supplies meet contract requirements at the manufacturer's location, observing manufacturing processes, examining products, and signing acceptance documentation that travels with the shipment. A sub-tier manufacturer subject to source inspection cannot ship without QAR acceptance.

2. Delegated Quality Authority: DCMA's quality assurance

role is triggered by inspection instructions issued by the activity responsible for technical requirements under DFARS PGI 246.103 (2).^[50] Those instructions must be prepared on a contract-by-contract basis, kept to a minimum, and tied directly to contract quality requirements. The PGI also prohibits instructions from substituting for incomplete contract quality requirements, imposing inspection requirements beyond those in the contract, or using broad designations such as "all characteristics." This means the instructions cannot expand on what the contract requires; they can only direct how DCMA verifies it. When DCMA is the administering office, it refers to those instructions as Quality Assurance Letters of Instruction (QALIs), described operationally in DCMA Manual 2303-01 Volume 7.^[51] Surveillance delegations between DCMA offices are governed by DCMA Manual 2101-04.^[52] The instructions determine what DCMA does at the manufacturer's facility, which is anything from periodic surveillance to first-article inspection witnessing to production lot testing. A manufacturer should know which contracts have these instructions and what they require.

3. Corrective Action Authority: When DCMA identifies

quality issues, the QAR can issue a Corrective Action Request (CAR) requiring the contractor to investigate root cause, implement corrective action, and document the response. Under DCMA-MAN 2303-05, CARs are issued at four severity levels: Level I for minor non-compliance correctable on the spot, with no root cause analysis required; Level II for systemic non-compliance requiring a written corrective action plan; Level III for serious non-compliance directed to top business management and potentially accompanied by contractual remedies (payment withholding, cost disallowance, business system disapproval); and Level IV when a Level III has failed or the non-compliance is severe enough to warrant immediate contractual remedies.^[53] CAR history factors into contractor performance evaluations under FAR Subpart 42.15, which contracting officers consider in future source selections.^[54]

4. DCMA Surveillance: Surveillance is the ongoing oversight

DCMA performs at contractor facilities, governed by DCMA Manual 2303-01 Volume 7.^[51] Surveillance ranges from kind-count inspections (verifying that shipped quantities match contract requirements) to full process surveillance (observing manufacturing operations, reviewing inspection records, and auditing the contractor's quality management system). The intensity depends on contract risk, prior performance history, and QALI scope. For sub-tiers, the takeaway is that DCMA presence on the shop floor is a continuous relationship that generates documentation reflecting on every future contract.

5. CPSR Threshold and Flow-Downs: As referenced earlier, under FAR Subpart 44.3, contractors with DOD sales exceeding \$25 million are subject to a CPSR where DCMA evaluates the contractor's purchasing system for effectiveness and adequacy. ^[42] For sub-tier manufacturers below the threshold, the obligation flows through prime contractor flow-down clauses under DFARS 252.244-7001, which require primes to flow purchasing system and quality requirements down through the supply chain. ^[38] A sub-tier manufacturer that grows past \$25M in DOD sales becomes directly subject to CPSR, and the purchasing practices established before that threshold become much harder to change once DCMA is reviewing them directly.

DCAA AUDITS: THE PROGRAMS THAT DEFINE COMPLIANCE

The DCMA oversight described above covers the shop floor. DCAA oversight covers the books, and DCAA publishes specific audit programs that define precisely what auditors test across labor, materials, accounting, indirect rates, and business system deficiency reporting. A sub-tier manufacturer that has reviewed these programs and configured systems accordingly will have fewer surprises when the audit arrives. DCAA updated this guidance in 2025.^[55]

Some of the programs most relevant to sub-tier manufacturers are:

- » 10310/13500: Labor floor check programs for non-major and major contractors.
 - **What DCAA tests:** Auditors arrive unannounced and physically verify that employees are charging labor to the correct cost objectives at the moment work is being performed. They interview employees, observe the work, and trace observations to the contemporaneous timekeeping record.
 - **Typical findings:** Employees unable to identify their charge code in real time; labor records modified after the fact without supporting documentation; timekeeping systems that permit bulk or retroactive labor allocation rather than enforcing point-of-entry assignment to a specific contract.
 - **How CTND addresses this:** Via the [CTND Government Accounting Service](#), we configure the Epicor ERP platform's timekeeping to enforce SF1408-aligned controls at the point of entry. This requires daily time submission rather than period-end reconstruction, capturing supervisor-initiated changes through an approval workflow that requires employee acknowledgment and a documented reason, and preserving the audit trail auditors expect to see during a floor check. Actual-time recording for exempt employees closes the gap that often surfaces when auditors trace observed work back to the labor distribution.
- » 12500ST and 12500FWU: MMAS compliance.
 - **What DCAA tests:** Whether material costs are based on valid time-phased requirements, whether the MMAS meets the 98 percent bill-of-materials, 95 percent master production schedule, and 95 percent inventory record accuracy thresholds under DFARS 252.242-7004, and whether common inventory used across contracts is allocated consistently.
 - **Typical findings:** Inventory record accuracy below threshold; inconsistent costing methodology across contracts; inability to demonstrate that material transferred between contracts was properly costed and authorized.

- **How CTND addresses this:** CTND Compliance Solution adds controls to prevent inaccurate inventory record creation and skewed material costs. Additionally, this solution aligns materials to contracts through flow downs, creating a permanent record that is part of the auditable genealogy.
- » 11070ST and 11070FWU: Accounting system audit.
 - **What DCAA tests:** DFARS 252.242-7006 criteria, including segregation of direct and indirect costs, identification and accumulation of costs by contract, a labor distribution system tied to cost objectives, and management reviews and reconciliations.
 - **Typical findings:** Commingled direct and indirect costs; indirect cost pools that don't reconcile to the general ledger; inability to produce contract-level cost reports without manual reconstruction.
 - **How CTND addresses this:** CTND configures Epicor's chart of accounts and cost structure to segregate direct from indirect costs, with unallowable costs isolated in dedicated accounts rather than commingled in general and administrative (G&A) expenses. Fringe, overhead, G&A, bid and proposal costs (B&P), and independent research and development (IR&D) are established as discrete pools with defined allocation bases, and Epicor captures applied rates that support reconciliation between indirect pool balances and the general ledger. The same configuration supports Incurred Cost Electronically (ICE) model reporting directly from Epicor data.
- » 10100 PYES/PYEL: Incurred cost submission and indirect rate audit.
 - **What DCAA tests:** Whether the annual incurred cost submission (due within six months of fiscal year-end) reconciles to the audited financial statements and general ledger trial balance, whether indirect cost pools are properly defined with allocation bases consistent with prior years and the Disclosure Statement, whether unallowable costs have been excluded from each pool against FAR 31 cost principles, and whether claimed rates match the actual costs in the general ledger (G/L). Executive compensation reasonableness against the FAR 31.205-6(p) benchmark, funded-when-paid treatment of paid leave, and fringe pool consolidation are tested within this audit.
 - **Typical findings:** Unexplained variances between claimed costs and G/L balances; unallowable costs included in indirect pools even when separately labeled, resulting in rate recomputation and **contract** debt determinations; G&A base changes year-over-year without Administrative Contracting Officer (ACO) notification, violating CAS 410 consistency requirements; B&P and IR&D costs not separately reported, preventing verification of FAR 31.205-18 and 31.205-48 cap compliance; revenue not broken out by contract type (cost-plus-fixed-fee, time-and-materials, firm-fixed-price), preventing auditors from reconciling billed amounts to cost pools by contract.
 - **How CTND addresses this:** CTND ensures your rates, pools, and cost submissions line up the way DCAA expects, so you're not scrambling to explain variances or fix unallowables after the audit starts.
- » 11090: Business system deficiency reporting used when material weaknesses are identified.
 - **What DCAA tests:** This is a reporting framework. When auditors identify material weaknesses across any of the six business systems, they apply the 11090 program to document the deficiency, the contractor's corrective action plan, and the basis for any payment withholding recommendation under DFARS 252.242-

7005. DCAA revised its business system audit guidance in May 2025, replacing the term “significant deficiency” with “material weakness” to align with the FY2021 NDAA and generally accepted government auditing standards.^[56]

- **Typical findings:** 11090 is the mechanism through which findings from the other programs become formal deficiency reports. A finding under 10310, 12500, 11070, or 10100 triggers an 11090 report that becomes the basis for withholding action.
- **How CTND addresses this:** CTND gets your systems running smoothly and consistently, reducing the chances that a DCAA finding turns into an 11090 deficiency report and a withholding recommendation.

A contractor who’s reviewed these programs has the diagnostic map. The configuration work that follows is what makes the map an operational reality.

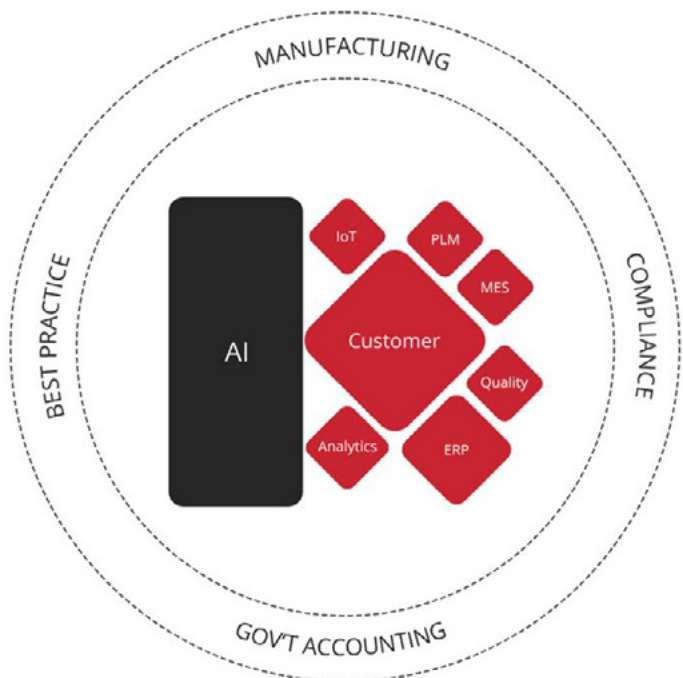
Configure ERP, Accounting, and Cybersecurity Controls for Defense

A defense-configured ERP serves as the system of record across the full production cycle — supplier data, inspection results, labor charges, material movements, and usage in final assemblies — and that’s what speeds regulatory reporting and reduces audit exposure.

“For many of our clients, these gaps surface during the first audit,” says Aronson. “The configuration decisions that matter most are the ones that happen before go-live. The manufacturers who move fastest are the ones who treat ERP configuration as part of their contract readiness, not as a back-office project they’ll get to later.”

This third playbook component is the one most manufacturers underestimate. Commercial ERP configurations were built for commercial requirements. Defense work requires specific configuration decisions that determine whether the system generates audit-ready evidence or requires manual reconstruction after the fact.

Configuration is where the readiness principle becomes a technical question. Labor charging, cost segregation, and inventory costing methodology either produce the evidence the auditor needs, or they don’t.



THE DEFENSE RAMP-UP IS HERE:

The three configuration decisions that most frequently determine audit outcomes are:

- » Labor charging configuration: The system must enforce the assignment of every labor hour to a specific contract or cost objective at the time of entry. A system that allows labor to be allocated retroactively or in bulk creates audit exposure regardless of how accurate the underlying records are. This requirement is tested directly in DCAA's accounting system audit program under DFARS 252.242-7006.^[28]
- » Cost segregation between direct and indirect costs: Direct costs charged to a specific contract must be cleanly separated from overhead and G&A expenses. Commingled costs are one of the most common material weakness findings DCAA identifies in accounting system audits.
- » Inventory costing methodology: The approach used to cost material transactions must be consistent across all contract and customer types and across accounting periods. Inconsistency in costing methodology triggers MMAS findings under DFARS 252.242-7004.^[27]

Configuring the system correctly from the start is faster and less expensive than remediating findings after the fact.

"Labor charging, cost pool structure, and inventory costing methodology: if set up correctly, the system automatically generates compliance evidence," says Aronson. "If they aren't, you're manually reconstructing records every time an auditor shows up. We can fix it after the fact, but it takes 6 to 12 months and costs the client in time and withheld payments."

**The configuration decisions that matter most
are the ones that happen before go-live.**

BOB ARONSON

Chief Revenue Officer, Cre8tive Technology and Design

A NOTE ON COST ACCOUNTING STANDARDS (CAS)

CAS compliance is a real concern for some defense contractors, but most sub-tier manufacturers entering the defense market won't be subject to it unless they take on a CAS-covered contract of \$7.5 million or more. The FY26 NDAA narrows applicability even further, effective June 30, 2026.^[26]

Small businesses are exempt regardless of contract size. For non-small businesses, CAS applicability depends on contract value and timing:

- **Contracts entered before June 30, 2026:** CAS applies to contracts above the Truth in Negotiations Act (TINA) threshold (currently \$2.5 million under FAR 15.403-4), with the \$7.5 million “trigger contract” exemption under 48 CFR §9903.201-1(b)(7) still in effect.^{[57][58][59]} Full CAS coverage under 48 CFR §9903.201-2(a) applies at \$50 million.^[57]
- **Contracts entered on or after June 30, 2026:** Under Section 1806 of the FY26 NDAA, CAS applies only to contracts of \$35 million or more.^[26] The trigger contract mechanism is eliminated. Full CAS coverage threshold rises to \$100 million.

Contracts for commercial items, firm-fixed-price contracts awarded without certified cost or pricing data, and contracts below the TINA threshold (currently \$2.5 million, rising to \$10 million after June 30, 2026) are also exempt.

For contractors who cross into modified CAS coverage, 48 CFR §9903.201-2(b) specifies four standards that govern day-to-day accounting^[57]:

- CAS 401 requires consistency between practices used to estimate costs for a proposal and practices used to accumulate and report those costs during performance.^[60]
- CAS 402 requires consistent treatment of costs incurred for the same purpose in like circumstances. A cost can't be charged as direct on one contract and indirect on another.^[61]
- CAS 405 governs the accounting treatment of unallowable costs, which must be identified and excluded from billings to the government.^[62]
- CAS 406 requires a consistent cost accounting period for accumulating and reporting costs.^[63]

For contractors who eventually reach full CAS coverage, two additional standards become operationally significant: CAS 410 governs the allocation of G&A expenses to final cost objectives, and CAS 418 governs the allocation of indirect costs based on beneficial or causal relationships.^{[64][65]}

For a growing sub-tier manufacturer, cost accounting practices established early — when CAS doesn't apply — become much harder to change once it does. A contractor crossing into modified or full CAS coverage triggers a Cost Accounting Standards Board Disclosure Statement requirement, and changes to disclosed practices after filing can trigger price adjustments to existing contracts.^[66]

CYBERSECURITY

CTND's most common finding is that manufacturers treat CMMC as an IT problem that can be addressed after contract award. CMMC is a business eligibility requirement that must be in place *before* the award.

"The most common cybersecurity misconception we encounter is that CMMC is an IT problem," says Aronson. "It's a business eligibility problem. If you handle CUI and aren't certified at Level 2 before the contract is awarded, you can't perform on it."

If you handle CUI and aren't certified at Level 2 before the contract is awarded, you can't perform on it. We've seen manufacturers lose awards they were otherwise qualified for because they discovered the cybersecurity requirement too late.

BOB ARONSON

Chief Revenue Officer
Cre8tive Technology and Design



The first practical step is determining whether your operation handles CUI or only Federal Contract Information (FCI). This distinction dictates which CMMC level applies and what assessment pathway is required. [CTND's CMMC readiness guide](#) breaks down the level determination and assessment process in detail:

- **Level 1 (Foundational):** Applies to contractors handling only FCI. Requires annual self-assessment and affirmation. Covers 17 foundational cybersecurity practices from the National Institute of Standards and Technology (NIST) Special Publication 800-171.^[67]
- **Level 2 (Advanced):** Applies to contractors handling CUI. Requires triennial third-party assessment by an accredited Certified Third-Party Assessor Organization (C3PAO). Covers 110 controls from NIST SP 800-171.^[67]
- **Level 3 (Expert):** Reserved for the most sensitive **DOD** programs. Requires a government-led CMMC compliance assessment. Covers controls from NIST SP 800-172.^[68]

If your shop produces components for aircraft, weapons systems, or other sensitive military technology, you're almost certainly handling CUI and will likely need Level 2 certification (typically by a C3PAO for DOD Organizational Index CUI). When CMMC is required by a solicitation, the required CMMC status must be in place at the time of contract award, though a Conditional status with an active Plan of Action and Milestones (POA&M) is acceptable at Levels 2 and 3 for a period not to exceed 180 days.^[36]

The path to Level 2 certification follows three phases:

- » Gap assessment: Map your current IT systems, network architecture, policies, and documentation against NIST and CMMC controls. Identify where you fall short.
- » Remediation: Close identified gaps, implement required technical and administrative controls, and train your team. Document everything.
- » Third-party assessment: Engage an accredited C3PAO to verify compliance. The assessment covers technical controls, administrative policies, and physical access.

Each phase generates documentation that becomes the basis for the assessment itself, most importantly the System Security Plan (SSP) and the POA&M discussed below.

“We’ve seen manufacturers lose awards they were otherwise qualified for because they discovered the cybersecurity requirement too late,” says Aronson. “The gap assessment and POA&M need to start the moment you decide you want to pursue defense work.”

Identifying CUI in Your Manufacturing Environment

Before a manufacturer can determine which CMMC level applies, it must identify which information in its environment qualifies as CUI under the federal CUI Program established by 32 CFR Part 2002.^[69]

CUI enters a sub-tier manufacturer’s environment in several common forms, like marked technical data from customers or primes (drawings, specifications, and engineering data carrying CUI markings or distribution statements), contracts containing DFARS 252.204-7012, derivative data the manufacturer creates from CUI inputs (a quote built around a CUI drawing is typically itself CUI), and information categories specified on the DD Form 254 for contracts involving controlled information.^[70] The full DOD index of CUI categories is maintained at the DOD CUI Registry, and the implementing policy is DOD 5200.48.^{[71][72]}

The complication is that DOD’s marking discipline has been inconsistent, so manufacturers can’t rely entirely on incoming markings. They must model how CUI flows through their environment based on contract scope, the technical work being performed, and the data exchanges happening with customers, primes, and sub-tier suppliers. A defensible CUI inventory documents what categories are involved in each contract, how CUI enters the environment, where it resides (ERP, file shares, and engineering workstations), who has access, and how it leaves — and that inventory is the foundation for every subsequent step.

Classifying Technical Data: ITAR, EAR, or Uncontrolled

Many sub-tier manufacturers assume export control classification has been handled upstream by the prime. It hasn’t fully. The prime classifies what it provides; the manufacturer is responsible for classifying everything it creates from that input, as well as everything it sends downstream to its own suppliers.

Classification follows a defined review order. Start with the USML under 22 CFR Part 121 (the ITAR order of review is in 22 CFR §120.11).^{[73][74]} If an item is enumerated on the USML or “specially designed” for a USML item, it is subject

THE DEFENSE RAMP-UP IS HERE:

to ITAR. If not on the USML, check the CCL under Supplement No. 1 to 15 CFR Part 774, using the CCL order of review in Supplement No. 4.^[46]

If on neither list, the item is generally EAR99 and faces fewer restrictions but still can't be exported to embargoed destinations or prohibited end users.^{[75][76]} When uncertain, a Commodity Jurisdiction (CJ) request to the State Department resolves USML vs. EAR jurisdiction, and a classification request through BIS's Commodity Classification Automated Tracking System (CCATS) resolves classification within the CCL.^{[77][78]} BIS publishes guidance on how the two orders of review fit together.^[79]

Three points are worth understanding before any drawing is classified. First, technical data has the same jurisdiction as the article it describes. A drawing for a USML item is itself USML, and sharing it with a foreign person inside the U.S. is a deemed export requiring authorization.^[80] Second, "specially designed" is a term of art with specific criteria under both regimes; a part isn't specially designed for a defense article simply because the manufacturer believes it is.^[81] Third, willful misclassification of ITAR-controlled technical data — or misclassification that enables an unauthorized export — carries criminal exposure under the Arms Export Control Act, with fines up to \$1 million per violation and up to 20 years imprisonment for the company and the individuals involved.^[82]

Manufacturers without in-house export control expertise should engage qualified counsel or specialized consultants for classification decisions, especially for first-of-its-kind items or anything bordering on USML categories.

Segregating CUI in the ERP and IT Environment

NIST SP 800-171 specifies the controls that must be applied to systems handling CUI, organized across 14 families covering access control, audit logging, configuration management, encryption, network protection, and others.

^[67] Applying these controls in a manufacturing environment means configuring the ERP and the broader IT environment to enforce several specific disciplines: logical separation of CUI from commercial data within ERP modules and file systems; access controls tied to authorized personnel with documented need-to-know (and to U.S. persons where ITAR applies); encryption in transit and at rest using Federal Information Processing Standards (FIPS)-validated cryptography; audit logging of system actions involving CUI; network segmentation isolating CUI systems from commercial-only workflows; and hardened endpoint configurations with current patching and monitoring.

The question for a sub-tier manufacturer is how to configure the specific ERP system to enforce them without breaking the production workflow.

Building Defensible SSP and POA&M Documentation

The SSP and POA&M are the two foundational documents in any CMMC assessment. The SSP describes how the manufacturer implements each applicable NIST SP 800-171 control; the POA&M tracks any gaps and the plan to close them.^[67] Both are required for Level 2 assessment, and both are reviewed by the C3PAO during certification.

NIST SP 800-171A defines what an assessor looks for: a clear description of the system boundary, an accurate

THE DEFENSE RAMP-UP IS HERE:

representation of each control's implementation, sufficient detail for the assessor to determine whether the control objective is met, and traceability between documented controls and the actual technical implementation in the environment.^[83]

COMPETITIVE ADVANTAGE: HOW READINESS WINS WORK IN RFP SCORING AND PRIME SELECTION

Every dollar spent on compliance infrastructure is also an investment in competitive positioning. Most sub-tier manufacturers don't think about it that way, but the government does. Under FAR 15.304, contract awards are based on evaluation factors tailored to the acquisition, and every source selection must address quality through non-cost factors, including past performance, technical excellence, and management capability.^[84] A manufacturer with auditable systems, documented traceability, and a clean compliance record demonstrates management capability and execution confidence before a proposal is even submitted.



"We had a machine shop client at \$1 million in government contracts," says Aronson. "They invested in a compliant ERP solution, built the systems, and went to market. Within the same year, they were at \$5 million. The government rewards the supplier it can trust to perform."

For major defense acquisition programs (MDAPs), the government goes further. DFARS 215.304 requires contracting officers to consider manufacturing readiness and manufacturing-readiness processes during source selection. Readiness is a named criterion.^[85] And under FAR 15.101-1, the government can award a contract to a proposal that isn't the lowest price if the trade-off yields greater overall value.^[86] A manufacturer that has invested in compliant systems is competing on a dimension where price isn't the only variable, and where an underprepared competitor at a lower price is a liability the evaluator must justify.

The implication runs in both directions. What evaluators score is the confidence that the supplier's system of record will hold up under audit. A manufacturer who has built that capability reduces risk for the prime and the contracting officer alike, which is what execution confidence means in defense source selection.

A supplier with approved business systems, a clean audit history, and documented quality controls is easier to onboard, easier to defend against the government, and less likely to generate mid-contract problems that reflect on the prime. Readiness reduces the prime's risk, which makes a ready supplier more valuable than a cheaper one who hasn't done the work.

Closing the Readiness Gap in Defense Manufacturing

The demand signal isn't slowing down, and the DOW's Acquisition Transformation Strategy makes the direction explicit. The U.S. DIB must prioritize schedule and volume, expand the industrial base, and award contracts directly to non-traditional suppliers throughout the supply chain. The government is inviting sub-tier manufacturers to fuel this expansion.

The manufacturers who will capture that opportunity are those whose systems of record already produce audit-ready evidence as a byproduct of daily operations, not those who will scramble to assemble it after the contract is won. For most sub-tier manufacturers, the readiness gap shows up in production scheduling that can't generate the documentation defense contracts require, accounting systems that weren't configured for government cost allocation, and a cybersecurity posture that has never been formally assessed. All these gaps are fixable, and the manufacturers who close them before the contract arrives close them on their own terms at lower cost, on their own timeline, and without the pressure of an active audit.

That's the practical case for treating readiness as an operating discipline rather than a compliance project. A system of record configured to satisfy DCAA, DCMA, and DFARS requirements is also a system of record that runs the business more cleanly: labor charged to the right contract at the point of entry, materials traceable from receipt through delivery, costs segregated and reportable on demand. The same discipline that satisfies an auditor satisfies a CFO, a customer, and a prime contractor flowing down requirements through the supply chain. Defense readiness, in other words, is operational excellence with documentation attached.

**The manufacturers we see succeed in defense [are]...
the ones who are honest about where they are, willing
to do the work and smart enough to start before the
government shows up.**

BOB ARONSON

Chief Revenue Officer, Cre8tive Technology and Design

"The manufacturers we see succeeding in defense aren't necessarily the most sophisticated operations when we first meet them," says Aronson. "They're the ones who are honest about where they are, willing to do the work and smart enough to start before the government shows up. If you're reading this and thinking about pursuing defense work, the best time to assess your readiness was six months ago. The second-best time is right now. We can tell you in one conversation what it'll take."

CTND's free business review is designed to help manufacturers understand exactly where they stand and build a practical roadmap for closing the gap.

[Schedule your free business review](#) with CTND. Our team will assess your current technology environment, identify your highest-leverage readiness gaps, and deliver a practical roadmap with timeframes and cost estimates so you can move into defense work on your terms.

Sources

1. <https://www.stripes.com/branches/army/2025-09-25/155mm-artillery-round-contract-639-million-19217101.html>
2. <https://www.whitehouse.gov/releases/2026/03/operation-epic-fury-unmatched-power-unrelenting-force-of-americas-warriors/>
3. <https://www.wsj.com/livecoverage/us-israel-iran-war-2026/card/rheinmetall-estimates-cost-of-u-s-munitions-used-in-first-three-days-Z0BNSOiZMP7u63R15qk6>
4. <https://www.defenseone.com/policy/2024/02/army-aims-double-155mm-shell-production-october/393943/>
5. <https://breakingdefense.com/2026/02/army-official-not-happy-with-gds-handling-of-155mm-contract-as-production-lags/>
6. <https://media.defense.gov/2026/jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF>
7. <https://www.federalregister.gov/documents/2025/06/04/2025-10322/presidential-waiver-of-statutory-requirements-pursuant-to-section-303-of-the-defense-production-act>
8. <https://media.defense.gov/2025/Nov/10/2003819439/-1/-1/1/TRANSFORMING-THE-DEFENSE-ACQUISITION-SYSTEM-INTO-THE-WARFIGHTING-ACQUISITION-SYSTEM-TO-ACCELERATE-FIELDING-OF-URGENTLY-NEEDED-CAPABILITIES-TO-OUR-WARRIORS.PDF>
9. <https://files.gao.gov/reports/GAO-25-108528/index.html>
10. <https://www.reuters.com/business/aerospace-defense/defense-executives-plan-meet-white-house-strikes-iran-diminish-stockpiles-2026-03-04/>
11. <https://www.nbcnews.com/politics/congress/first-6-days-iran-war-cost-11-billion-pentagon-tells-senators-rcna263060>
12. <https://breakingdefense.com/2026/03/hegseth-confirms-potential-200-billion-request-for-iran-operations-but-figure-could-move/>
13. <https://www.washingtonpost.com/national-security/2026/04/07/trump-iran-war-funding/>
14. <https://www.cbsnews.com/news/congress-returns-iran-war-dhs-shutdown/>
15. <https://www.npr.org/2026/04/12/nx-s1-5782538/u-s-iran-peace-talks-islamabad-collapse>
16. <https://www.whitehouse.gov/presidential-actions/2025/04/modernizing-defense-acquisitions-and-spurring-innovation-in-the-defense-industrial-base/>
17. <https://media.defense.gov/2025/Nov/10/2003819441/-1/-1/1/ACQUISITION-TRANSFORMATION-STRATEGY.PDF>
18. <https://www.whitehouse.gov/briefings-statements/2026/02/congressional-bill-h-r-7148-signed-into-law/>
19. <https://www.appropriations.senate.gov/news/majority/congress-approves-fy-2026-defense-appropriations-bill>
20. <https://media.defense.gov/2025/Nov/10/2003819439/-1/-1/1/TRANSFORMING-THE-DEFENSE-ACQUISITION-SYSTEM-INTO-THE-WARFIGHTING-ACQUISITION-SYSTEM-TO-ACCELERATE-FIELDING-OF-URGENTLY-NEEDED-CAPABILITIES-TO-OUR-WARRIORS.PDF>
21. <https://www.airandspaceforces.com/pentagon-industrial-base-reforms-report/>
22. <https://www.gao.gov/assets/gao-25-107283.pdf>
23. <https://docs.house.gov/meetings/AS/AS25/20250611/118370/HMTG-119-AS25-Wstate-MoraniS-20250611.pdf>
24. https://dbb.defense.gov/Portals/35/Documents/Reports/2025/Industry%20Partnerships%20for%20Crises%20Study%20Report_CLEARED_%2022%20Nov_red.pdf
25. <https://rsmus.com/insights/industries/government-contracting/takeaways-from-fiscal-year-2025-national-defense-authorization-act.html>
26. <https://www.congress.gov/bill/119th-congress/senate-bill/2296>
27. <https://www.acquisition.gov/dfars/252.242-7004-material-management-and-accounting-system>
28. <https://www.acquisition.gov/dfars/252.242-7006-accounting-system-administration>
29. <https://www.acquisition.gov/dfars/252.242-7005-contractor-business-systems>
30. https://www.acquisition.gov/far/16.104#FAR_16_104
31. <https://www.dcaa.mil/Checklists-Tools/Pre-award-Accounting-System-Adequacy-Checklist/>
32. <https://www.dcaa.mil/Portals/88/FY%202025%20Management%20Discussion%20and%20Analysis.pdf>
33. <https://www.pilieromazza.com/cybersecurity-compliance-in-the-crosshairs-raytheon-8-4-million-fca-settlement-and-what-it-means-for-defense-contractors-2/>
34. <https://www.justice.gov/opa/pr/california-defense-contractor-and-private-equity-firm-agree-pay-175m-resolve-false-claims>
35. <https://www.mintz.com/insights-center/viewpoints/2406/2026-01-13-cybersecurity-related-enforcement-under-false-claims-act>
36. <https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of>
37. <https://www.acquisition.gov/far/52.244-6>
38. <https://www.acquisition.gov/dfars/252.244-7001-contractor-purchasing-system-administration>
39. <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-A/part-700>
40. <https://www.acquisition.gov/far/52.209-3>
41. <https://www.acquisition.gov/far/46.315>

42. <https://www.acquisition.gov/far/subpart-44.3>
43. <https://www.acquisition.gov/dfars/252.209-7004-subcontracting-firms-are-owned-or-controlled-government-country-state-sponsor-terrorism>
44. <https://www.acquisition.gov/far/subpart-9.4>
45. <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120>
46. <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-774>
47. <https://www.acquisition.gov/far/part-42>
48. <https://www.acquisition.gov/far/46.402>
49. <https://www.acquisition.gov/dfars/246.103-contracting-office-responsibilities>
50. https://www.acquisition.gov/dfarspgi/pgi-246.103-contracting-office-responsibilities.#DFARS_PGI_246.103
51. https://www.dcmamail.com/Portals/31/Documents/Policy/DCMA_MAN_2303-01_VOL7.pdf
52. https://www.dcmamail.com/Portals/31/Documents/Policy/DCMA_MAN_2101-04.pdf
53. https://www.dcmamail.com/Portals/31/Documents/Policy/DCMA_MAN_2303-05.pdf
54. <https://www.acquisition.gov/far/subpart-42.15>
55. <https://www.dcaa.mil/Guidance/Directory-of-Audit-Programs/>
56. <https://www.dcaa.mil/Portals/88/Documents/Guidance/MRDs/25-PSC-001%28R%29.pdf?ver=BFiqrBmavk4%3D>
57. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9903/subpart-9903.2/section-9903.201-2>
58. <https://www.acquisition.gov/far/15.403-4>
59. <https://www.law.cornell.edu/cfr/text/48/9903.201-1>
60. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9904/section-9904.401>
61. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9904/section-9904.402>
62. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9904/section-9904.405>
63. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9904/section-9904.406>
64. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9904/section-9904.410>
65. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9904/section-9904.418>
66. <https://www.ecfr.gov/current/title-48/chapter-99/subchapter-B/part-9903/subpart-9903.2/section-9903.202-1>
67. <https://csrc.nist.gov/pubs/sp/800/171/r3/final>
68. <https://csrc.nist.gov/pubs/sp/800/172/r3/final>
69. <https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002>
70. <https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>
71. <https://www.dodcui.mil/>
72. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF>
73. <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121>
74. <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-B/section-120.11>
75. <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-746>
76. <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744>
77. <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-B/section-120.12>
78. <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-748/section-748.3>
79. <https://www.bis.gov/media/documents/ccl-order-review-faqs.pdf>
80. <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.50>
81. <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/>
82. <https://www.law.cornell.edu/uscode/text/22/2778>
83. <https://csrc.nist.gov/pubs/sp/800/171/a/r3/final>
84. <https://www.acquisition.gov/far/15.304>
85. <https://www.acquisition.gov/dfars/215.304-evaluation-factors-and-significant-subfactors>
86. <https://www.acquisition.gov/far/15.101-1>