GARRETT PARTRIDGE

OPERATIONS ARCHITECT

MARKET ENTRY

The US Market-Entry Playbook for Allied Defense Manufacturers

The operational stand-up sequence for a qualifying-country manufacturer building a compliant US defense operation, FOCI and ITAR posture included.

White Paper · Garrett Partridge · July 16, 2026

garrettpartridge.com · Brookline, NH

THE DIRECT ANSWER

An allied manufacturer wins Department of Defense work by standing up a real US operation, not by shipping across a border. Four things have to exist: a US entity, a US-person data boundary that keeps controlled technical data inside the American operation, an IT and OT environment built to a CMMC Level 2 and ITAR-ready posture, and an operating model that runs the floor to those standards from the first day it opens. Qualifying-country status under a reciprocal defense-procurement agreement gives your end products a procurement preference against Buy American restrictions. It waives nothing. ITAR, CMMC, and FOCI apply in full to a foreign-owned US operation, and building for them is the work. Only the first of the four is a legal filing. The other three are an operation, which is exactly where the advisors stop.

What you are actually building

You have US defense revenue you cannot capture from abroad. A prime wants the part built here. A program carries a domestic-content threshold. The technical data cannot leave a US-person boundary. Whatever the trigger, the answer is the same shape: a real US operation, standing and running to a standard an assessor will accept.

That operation is four things, and they come up together. Most parents discover them in the wrong order, one at a time, each one arriving as a surprise that resets the schedule.

- A US entity. The legal instrument your corporate counsel forms. Necessary, and the easiest of the four by a wide margin.
- A US-person data boundary. The controls that keep controlled technical data inside the American operation and govern every release out of it, including releases to your own parent.
- An IT and OT environment at a CMMC Level 2 and ITAR-ready posture. Not a data room bolted onto a shop floor. The floor itself, the ERP, the MES, and the test equipment, scoped and built as one auditable thread.
- An operating model. The org, the value stream, the SQDIP cadence, and the standard work that makes the other three hold on a Tuesday in month nine, when nobody is watching and the auditor is a year away.

> **The first is a filing. The other three are an operation. A US market-entry build is an operations problem wearing a compliance costume, and that is why the firms who show up to help keep handing you paper.**

Six advisors, and none of them owns the floor

Ask the market who helps a foreign manufacturer build a compliant US operation and you get six answers. Every one of them is real, competent, and worth paying. Every one of them stops at the same place.

- Market-entry and export-control law firms form the entity, file the DDTC registration, and negotiate the FOCI mitigation instrument with DCSA. They draft the agreement. They do not scope your CUI enclave or walk your floor.
- Big-4 and CFIUS advisory model the tax, the transfer pricing, and the structure of the inbound investment. They do not convert the resulting entity into a running, assessed shop floor.
- Site-selection consultancies deliver a building and an incentives package. Nobody in that tier operates inside the four walls afterward.
- SelectUSA and the state economic development offices recruit you and soften the landing on the government's dime. They are the best free help you will get, and they say plainly that they do not embed as your operating executive. I work alongside them.
- Aerospace and defense strategy advisors tell you whether to build, buy, or partner. They do not implement the build they recommend.
- CMMC and ITAR IT vendors sell you an enclave, a data room, or a path to a certificate. That product is often the right product. It is not an operation, and it does not know what your floor does.

> **Line the six tiers up in sequence: legal instrument, deal structure, location, incentives, sector strategy, compliance tooling. Then the sequence ends, and someone still has to stand up and run the operation. That last step is the one with no vendor. It is the lane I work in.**

The seam is where the schedule dies

Most parents solve the missing step one of two ways. They hire a US-subsidiary general manager and hope, which asks one person to simultaneously learn ITAR, scope a CMMC assessment, hire a floor, and hit a prime's date. Or they split the problem between the law firm and the IT vendor and let the seams fall where they fall.

The seams are the whole problem. Your counsel scopes the ITAR boundary in a memo. Your IT vendor scopes the enclave around the systems it was shown. Nobody notices that the drawing also lives on a CNC controller, in the quality lab, and on the laptop your test engineer takes to the customer site, because no one in the room has ever owned a floor. The assessment finds it, or worse, it does not, and the next audit does.

One planning note belongs to that second tier and gets missed. A greenfield build, a new US facility you stand up yourself, currently sits outside CFIUS jurisdiction, which reviews acquisitions of existing US businesses and certain real estate. Buying an existing US shop puts CFIUS in play. That is a live input to your build-versus-buy decision, and it is not permanent: the 2025 America First Investment Policy memo signaled that greenfield authority may expand. Your counsel tracks

it. I raise it because parents make the build-versus-buy call on cost and schedule, and then meet the review.

I am the operating layer. Everything below is what that layer actually does, in the order it has to happen.

Know your work class before anyone quotes you a timeline

Three classes of defense work exist. Each is a different build, a different cost, and a different calendar. A quote that does not name your class is a guess wearing a number.

- Class A, commercial and uncontrolled. Dual-use and commercial parts with no controlled technical data. Needs a US entity and a clean quality system. No CMMC boundary, no ITAR registration. Most parents reach this class on their own.
- Class B, CUI and ITAR-controlled but unclassified. The bulk of sub-tier DoD manufacturing. Needs DDTC registration, a US-person data boundary, and CMMC Level 2 built into the workflow. Achievable for a foreign-owned US entity without a facility clearance. This is the class I build and run.
- Class C, classified. Work that touches classified information. Needs a facility clearance and FOCI mitigation negotiated with DCSA. That is counsel and DCSA territory. I coordinate with your cleared-facility counsel; the clearance stays with them.

> **Class B is where a foreign-owned US operation lives, and it is reachable without a facility clearance. Parents who assume otherwise budget for a clearance program they do not need and delay a build they could already be running.**

Your product does not decide your class. Your data does.

The trap is reading your class off your product catalog. It does not work that way. Controlled technical data, not the visible part, is what pulls you into Class B. A high-reliability pressure sensor is a commercial component right up until its design data is specified into a DoD platform, and then it is not, and nothing about the sensor changed.

DFARS 252.204-7012 defines controlled technical information as technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Read that list of verbs again, slowly. Access. Use. Reproduction. Modification. Display. Every one of them is something your engineers do a hundred times a day, on the floor, in the ERP, on the test bench, at 200 percent zoom on a shop-floor monitor.

This is why the compliance boundary cannot be drawn by someone who has only seen your org chart. It has to be drawn by someone who knows where the drawing actually goes once a machinist opens it.

Qualifying country is a procurement preference, not a shortcut

Canada, the United Kingdom, Germany, Italy, France, Japan, Australia, Spain, and Switzerland are all DFARS qualifying countries. So are Belgium, Denmark, Finland, the Netherlands, Norway, Poland, Sweden, and a dozen others. The list lives at DFARS 225.003, and it is the receipt behind the word allied.

The status does one thing. Under a reciprocal defense-procurement memorandum of understanding with the Department of Defense, qualifying-country end products and components receive a procurement preference against Buy American restrictions. That is real, it is valuable, and it is the reason your country is on my list at all.

What it does not do is the part that decides your build. Qualifying-country status does not waive ITAR. It does not waive CMMC. It does not clear FOCI. It does not move one byte of controlled technical data across the Atlantic or across the 49th parallel. Those regimes apply to a German-owned US operation exactly as they apply to a family-owned shop in Nashua.

I put this early because everything downstream depends on it. A parent that reads qualifying country and hears reduced compliance burden budgets for the wrong build, staffs for the wrong build, and finds out when the prime's flowdown arrives with a date attached.

Country-specific nuance sits on top of this, and it is real. AUKUS Pillar 2 is lowering export-control friction between the UK, the US, and Australia while significant carve-outs remain. Canada sits closest of any ally, and the regulation says so in its own words: for production planning purposes, Canada is part of the defense industrial base (DFARS 225.870-1). The same section routes contracting with Canadian contractors through the Canadian Commercial Corporation, which awards and administers those contracts subject to four named exceptions. France sits outside AUKUS and runs the standard regime. Each of those changes what crosses a border. None of them changes what you build once you are here.

> **Qualifying-country status is a procurement preference, not a shortcut. It does not waive ITAR, it does not waive CMMC, and it does not clear FOCI. Those regimes still apply, and building for them is the work.**

The US-person data boundary is the build

Everything above is procurement. This section is criminal law, and it is where a foreign-parented operation actually gets hurt.

Start with the good news, because most parents have this backwards. Under ITAR, a US person includes any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated to do business in the United States. Your US subsidiary, once incorporated to do business here, is a US person. Foreign ownership does not change that. The entity is not the problem.

The people are. ITAR defines an export to include releasing or otherwise transferring technical data to a foreign person in the United States, and names that a deemed export. It goes further. Any release in the United States of technical data to a foreign person is deemed to be an export to

all countries in which the foreign person has held or holds citizenship or holds permanent residency.

Now read that against your actual org chart. Your US entity is a US person. The German engineer it employs in Massachusetts is not. Handing that engineer a controlled drawing is an export to Germany, performed in a conference room off Route 495, with no package, no border, and no customs form. Your parent's CTO reviewing a design over video from Brescia is an export to Italy. Your group ERP, replicating that drawing to a server in Frankfurt on the nightly sync, is an export every night at 2 a.m., automatically, whether or not a human ever opens the file.

That is why the US-person data boundary is a build and not a policy. A policy says the parent should not access controlled data. A boundary makes the access technically impossible except through an authorized path, and produces the evidence that it was. Identity and access management, network segmentation, ERP and PLM scoping, MES and test-equipment isolation, and a documented release process that puts a named human decision in front of every transfer out of the boundary.

The Canadian exemption at 22 CFR 126.5 produces the sharpest version of this misconception, and it earns a paragraph. It authorizes license-free export of certain unclassified USML items from the US to a Canadian-registered person. It carries real limits, including items excluded by Supplement No. 1 to Part 126 and prior DDTC approval for reexport or retransfer. It is a US-to-Canada export authorization. It is not a general license for a Canadian parent to reach into its US subsidiary's controlled technical data. Reading it that way is how a Canadian-parented operation ends up drafting a voluntary self-disclosure.

Transfers to the parent happen under DDTC authorization or not at all. That is not a policy position I am asking you to adopt. It is the design constraint the entire IT and OT architecture gets built around, and it is the first thing I set, because every later decision inherits it.

> **Your US entity is a US person the day it is incorporated. The individual foreign nationals inside it are not, and neither is your parent. The boundary is not between companies. It is between people, and it runs straight through your ERP.**

The registration line nobody reads

One line in the ITAR catches foreign-parented manufacturers who did not think the ITAR applied to them yet.

22 CFR 122.1 requires any person who engages in the United States in the business of manufacturing or exporting or temporarily importing defense articles, or furnishing defense services, to register with the Directorate of Defense Trade Controls. Then it adds the sentence people skip: a manufacturer who does not engage in exporting must nevertheless register.

You do not have to export anything. You do not have to ship a part, transfer a drawing, or intend to. If your US operation manufactures a defense article, you register. The regulation is explicit that engaging in that business requires only one occasion of manufacturing.

And registration is not authorization. The rule says so in its own words: registration does not confer any export rights or privileges. It is primarily a means to provide the US Government with

necessary information on who is involved in certain manufacturing and exporting activities, and it is generally a precondition to the issuance of any license or other approval. Parents routinely read a completed registration as a green light. It is a prerequisite to asking for one.

The rule carries narrow exemptions, including one for persons who engage in the fabrication of articles solely for experimental or scientific purposes, which is where a prototype-stage operation sometimes sits for a while. It is narrow, it stops applying the moment you are building for a program, and your export-control counsel makes that call, not me.

Your counsel files the registration. I make sure the operation the filing describes is the operation you are actually running, because a registration that describes a fiction is worse than no registration at all.

> **A manufacturer who does not engage in exporting must nevertheless register. That is the text of 22 CFR 122.1, and it reaches your US operation the first time it manufactures a defense article, whether or not anything ever leaves the country.**

The CMMC obligation is a contract clause, not a calendar

CMMC stopped being a policy conversation and became a clause. DFARS 252.204-7021 requires a contractor to have and maintain, for the duration of the contract, a current CMMC status at the level the contracting officer specifies, for all information systems used in performance that process, store, or transmit federal contract information or CUI. It requires an annual affirmation of continuous compliance by a named affirming official in SPRS. And it requires you, before awarding a subcontract, to confirm your own subcontractor's status. No status, no award. No affirmation, no continuation.

The phase-in is defined in the CMMC program rule at 32 CFR 170.3, and it runs in four one-year steps. Phase 1 begins on the effective date of the complementary 48 CFR CMMC acquisition final rule. That rule, DFARS Case 2019-D041, was published on September 10, 2025 and took effect on November 10, 2025. Phase 2 begins one calendar year following the start date of Phase 1, and Phase 2 was the step that would have made a CMMC Status of Level 2 with a certified third-party assessment a condition of contract award.

Then the program moved, and the regulation did not. On July 13, 2026, the Department suspended the Phase II requirements originally scheduled for November 10, 2026, established a CMMC reform task force, and left implementation paused in Phase 1. No replacement date has been named. As of July 2026, CMMC Level 2 is reached by a self-assessment every three years against the 110 security requirements in NIST SP 800-171 Revision 2, with an annual affirmation into SPRS, and the Department has said it will enforce through self-assessments and select government-led assessments during the review. The Phase I requirements remain, in the Department's own words, firmly in place. Read the rule and you get a schedule. Read the program and you get the truth, and this document is written for people who have to act on the second one.

Now read the suspension for the part the headline skipped, because that is the part that decides your build. The Department stated in terms that this action does not eliminate the requirement for companies to protect information in accordance with DFARS clause 252.204-7012. The certificate

was suspended. The obligation was not. The clause is still in your contract, the 110 requirements are still the standard, and your prime still cannot award you covered work unless your assessment is current, which is the gate DFARS 252.204-7020(g)(2) puts in front of the buyer deciding who it trusts with controlled technical data.

That is a harder deadline than November was, not a softer one. A date invites a parent to schedule the work for October. What replaced it does not wait: the clause binds today, and the assessment is now your own organization's statement to the government rather than an assessor's finding. Your government-contracts counsel owns that statement's legal exposure. I own whether the floor actually runs the controls you affirm. And note where the reform is aimed, because it is not where the compliance vendors are pointing: lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures. A review pointed at real cybersecurity instead of administrative overhead does not rescue an operation that bought a binder. It rewards the one that built the floor.

Level 2 is not a bespoke DoD invention. 32 CFR 170.14 states it plainly: the security requirements in CMMC Level 2 are identical to the requirements in NIST SP 800-171 R2. If your parent runs a mature ISO 27001 program, that discipline helps. It does not map one to one, because 800-171 scopes to wherever CUI actually lives, and in a manufacturing operation CUI lives on the floor.

Then there is the clause that decides whether your parent's IT department stays in the picture at all. DFARS 252.204-7012 requires that if you use an external cloud service provider to store, process, or transmit covered defense information, that provider must meet security requirements equivalent to those established by the Government for the FedRAMP Moderate baseline, and must comply with the clause's incident reporting, media preservation, and forensic access obligations. Your group's European tenant. Your parent's shared ERP instance. The PLM your engineering organization runs globally, the one your CTO will absolutely assume the US site will just connect to. Each of those is in scope the moment it touches covered defense information, and most of them do not clear that bar.

The same clause defines a covered contractor information system as an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. That definition does not say office IT. If the drawing is on the CNC controller, the controller is in scope. This is the entire argument for converging IT and OT before the assessment instead of after it, and it is why an enclave sold as a compliance solution can leave your floor sitting outside the boundary it was bought to protect.

And the clause has a stopwatch in it. Rapidly report means within 72 hours of discovery of any cyber incident, filed with DoD through the DIBNet portal, which requires a DoD-approved medium assurance certificate you have to obtain before you need it rather than during. A parent whose incident response routes through a European SOC, a group legal review, and a time zone will not make 72 hours on the day it counts.

> Anchor to the clause, not the calendar. On July 13, 2026 the Department suspended the Phase II certification requirement and named no replacement date. DFARS 252.204-7012 did not move an inch. An operation built to the 110 requirements is ready for whatever the reform returns. An operation that was counting down to November has nothing to show for the wait.

FOCI reshapes the org chart, not just the paperwork

Foreign Ownership, Control, or Influence is the regime that decides whether a foreign-owned US entity can hold a facility clearance. It is administered by the Defense Counterintelligence and Security Agency. DCSA is the referee. It is not a vendor, and no operator negotiates with it.

First the scoping question, because it saves this audience real money. A facility clearance and FOCI mitigation attach to classified work, which is Class C. If your US operation is doing Class B work, controlled technical data and CUI without classified information, you are very likely outside the facility-clearance path entirely. Confirm that with counsel rather than assuming in either direction: parents both over-budget for clearance programs they will never need, and get surprised when a specific customer or program raises foreign-ownership questions on unclassified work.

Where it does apply, the thing to understand is that FOCI mitigation is not a document you sign and file. The instruments DCSA uses, board resolutions, security control agreements, special security agreements, proxy arrangements, reach directly into how your company is governed. Who sits on the board. Which of your own executives may be briefed on what. Which reports flow to the parent and which stop at the US border. Who at the parent may direct the US entity's operations, and who may not.

Your counsel drafts that instrument. I live in its consequences. A special security agreement that walls the parent off from the subsidiary's technical operations is a legal document on Tuesday and an operating model on Wednesday: a reporting line that has to actually exist, a data flow that has to actually stop, an executive who genuinely cannot see a number they have reviewed every month for a decade. Building an operation that satisfies the instrument and still ships product is the work, and it is not legal work.

The published guidance here is thin and written for lawyers. DCSA documents the regime. The Center for Development of Security Excellence publishes a student guide. The DoD CIO's Standards Guide for Foreign Partners is a controls overlay. Not one of them tells you what to do with your org chart on Monday morning.

> FOCI mitigation is a legal instrument with an operating shadow. Your counsel owns the instrument. The shadow, the reporting lines, the data flows, and the daily reality of who can see what, is mine.

The 90-day operating build

The build runs in parallel, not in sequence, because a prime gate does not wait for you to finish one phase before starting the next. The operating model, the IT and OT environment, and the compliance posture come up together.

- Days 1 to 30, diagnostic and design. Stand up the US operating model on paper and on the floor: the org, the value stream, the SQDIP cadence, and the US-person data boundary your ITAR scope actually needs. Name your work class with your counsel. Scope the CUI enclave before anyone buys a tool.
- Days 30 to 60, stabilize and build. Bring the IT and OT environment to a CMMC and ITAR-ready posture from day one rather than retrofitted later. Scope the enclave tight so the assessment stays sane, and govern the parent's access by design instead of by exception.
- Days 60 to 90, qualify and run. Sequence the readiness evidence against the prime gate you are actually racing, coordinate the FOCI and DDTC steps with your counsel, and hand your team a floor that holds after I step back.

> **Ninety days gets the operation standing, running, and evidence-ready at a CMMC and ITAR-ready posture. It does not get you a status determination. As of July 2026 Level 2 runs on a self-assessment every three years and an annual affirmation into SPRS, and the reform task force may move that mechanism again. I sequence the readiness evidence toward whichever mechanism is in force when your gate arrives. Anyone who sells you a certification date is selling you a date they do not control, and in July 2026 the Department proved it.**

Why the quarter is possible at all

What makes a quarter realistic is doing the four builds concurrently instead of serially, and knowing the dependencies well enough to start the right thing on day one.

The serial version is the one I get called into. Form the entity. Then pick the site. Then hire a general manager. Then discover the ITAR scope. Then call an IT vendor. Then find out the enclave does not cover the shop floor. Then rescope the assessment, which moves the prime gate, which moves the hiring plan. That version does not have a duration. It keeps discovering its own requirements, and every discovery resets something upstream.

The parallel version front-loads the two decisions everything else inherits: your work class, and where the data boundary falls. Get those right in the first thirty days and the rest is execution against a known shape. Get them wrong and no amount of speed later recovers it.

The sequence is the deliverable. Not the checklist, not the enclave, not the report. The order.

Where you land

New England is the landing zone. Not because I am here, though I am, in Brookline, New Hampshire. Because the primes, the sub-tier supply base, and the compliance depth are already here, and a supplier standing up within driving distance of the line it feeds is worth something that does not show up in a site-selection spreadsheet.

The pattern is proven at both ends of the scale. In April 2026, American Rheinmetall, the US subsidiary of the German group, achieved CMMC Level 2 certification across its US production facilities. That is the large-cap version of this exact build, and it is a public, dated fact you can check yourself before you call me.

At the other end, GEFRAN, an Italian sensor and automation multinational, manufactures in North Andover, Massachusetts, less than an hour from my base. GEFRAN is not a defense supplier, and that is precisely the point: this corridor already holds European precision manufacturers running real US plants. The defense build is a posture added to a pattern that is already here and already working.

I ran GEFRAN's North America operations. I have been the foreign parent's operator in the United States, standing on the exact ground an Italian or a German parent is walking onto. And I am doing it now, standing up US defense manufacturing operations for a Canadian-parent subsidiary. The sequence in this document is the engagement I am running, not a framework assembled for a brochure.

The case for the corridor specifically, the prime density, the supplier base, the labor pool, and the reasons a Brescia or an Ontario parent lands here rather than in a lower-cost state, is the subject of The New England Landing Zone. The architecture of the data boundary itself, the digital thread that has to satisfy an ITAR data border and a CMMC assessment at the same time, is the subject of One Thread, Two Flags. The country lanes, Canada's CCC channel, the AUKUS carve-outs, the Mittelstand path, are taken apart one at a time in the market-entry briefs.

What I own, and what stays with your counsel

I stand up and run the compliant US operation: the floor, the operating model, the IT and OT build, the US-person data boundary, and the readiness evidence for the gate you are racing. Entity formation, FOCI mitigation, and site selection stay with your corporate counsel, your export-control counsel, and a site-selection advisor. I coordinate with them and own the operating outcome.

That boundary is deliberate, and it is the reason the engagement works. You already have advisors for the legal instrument, and none of them is going to run your floor. A firm that claims all of it is claiming a legal practice it does not have, and this audience checks.

What I add is the layer the six tiers leave open. An engineer who has operated: a manufacturer's CEO who signed the front of a paycheck, a general manager of a foreign subsidiary's North America operations, an operator who sat in the AS9100 audit chair rather than reviewing it from a slide, and who ran an MRP cutover on a live floor without losing a shipment.

The engagements are the existing three. A 30-Day Operational Triage that produces a defensible written plan rather than a deck. A Fractional COO retainer that embeds the operating leadership

through the build. A Strategic Consultancy scoped firm-fixed-price against one defined event. A market-entry build usually opens with the triage and continues as fractional leadership through the first ninety days, because that is when the decisions that cannot be undone get made.

A maximum of four concurrent engagements. Capacity is the constraint and the proof, because four is the real limit of doing this work at the depth it requires. Every engagement is held under NDA.

> **Name your trigger: a prime's interest you cannot serve from abroad, a program with a domestic-content threshold, a CMMC flowdown you cannot answer, or a US site decision already made. You get a realistic timing window within 48 hours.**

FREQUENTLY ASKED

Do we need a US entity, or can we sell to the Department of Defense from abroad?

Both are real paths, and the program decides which one you are on. Qualifying-country status gives your end products a procurement preference, and some channels let you sell without incorporating, most notably the Canadian Commercial Corporation, which can act as prime contractor into the DoD on behalf of Canadian firms. You stand up a US operation when a program needs controlled technical data held inside a US-person boundary, when a domestic-content or Buy American threshold applies, or when a prime expects its sub-tier supplier to have a real US footprint near the line. Those are the cases onshoring solves and a cross-border sale does not.

Does qualifying-country status exempt us from ITAR or CMMC?

No. All nine countries I serve are DFARS qualifying countries under reciprocal defense-procurement agreements, and that status gives your end products a procurement preference against Buy American restrictions. It is not an ITAR exemption, a CMMC exemption, or a FOCI clearance. Those regimes apply to a foreign-owned US operation in full. The qualifying-country list at DFARS 225.003 is a procurement document, not a compliance one, and reading it as a compliance discount is the most common budgeting error at this stage.

Our parent's engineers need access to the design data. Can they have it?

Only under authorization, and the rule is stricter than most parents expect. ITAR treats releasing technical data to a foreign person inside the United States as a deemed export, and any release to a foreign person is deemed an export to every country in which that person holds or has held citizenship or permanent residency. Your US entity is a US person once it is incorporated to do business here. The individual foreign nationals inside it, and your parent, are not. So a design review over video with headquarters is an export. Transfers to the parent happen under DDTC authorization or not at all, and the data boundary is what makes that enforceable rather than aspirational.

Do we have to register with DDTC if we never export anything?

Yes, if your US operation manufactures a defense article. 22 CFR 122.1 says it directly: a manufacturer who does not engage in exporting must nevertheless register. The same section notes that engaging in that business requires only one occasion of manufacturing. And registration is not permission. The rule states that registration does not confer any export rights or privileges; it is generally a precondition to asking for a license. Narrow exemptions exist, including one for fabrication solely for experimental or scientific purposes, and your export-control counsel makes that call, not your operator.

CMMC Phase II was suspended. When does Level 2 actually become mandatory?

The certification phase was suspended. The requirement was not. On July 13, 2026 the Department suspended the Phase II requirements originally scheduled for November 10, 2026, established a reform task force, and left implementation paused in Phase 1, with no replacement date named. What moved is the assessment mechanism: as of July 2026, CMMC Level 2 is reached by a self-assessment every three years against the 110 security requirements in NIST SP 800-171 Revision 2, with an annual affirmation into SPRS. What did not move is the obligation. The Department stated that the action does not eliminate the requirement for companies to protect information in accordance with DFARS clause 252.204-7012. That clause is in your contract now, it flows down to your subcontractors now, and your prime cannot award you covered work now unless your assessment is current, the gate DFARS 252.204-7020(g)(2) puts in front of them. Build the floor to the 110 requirements and you are ready for whatever the task force returns. Wait for a date and you are waiting on a program that just withdrew one.

Can our US site just connect to the parent's ERP and PLM?

Usually not, and this is the assumption that breaks the most build plans. DFARS 252.204-7012 requires that any external cloud service provider storing, processing, or transmitting covered defense information meet security requirements equivalent to the Government's FedRAMP Moderate baseline and comply with the clause's incident reporting and forensic access obligations. A group tenant hosted in Europe rarely clears that. Separately, every replication of controlled technical data to a parent-side server is a release to a foreign person, which ITAR treats as an export. The answer is not always a full split, but it is always a scoping decision made before the integration is built, not after.

Do we need a facility clearance and FOCI mitigation?

Probably not, if your work is unclassified. A facility clearance and FOCI mitigation negotiated with DCSA attach to classified work. The bulk of sub-tier DoD manufacturing is CUI and ITAR-controlled but unclassified, and a foreign-owned US entity can reach that class without a facility clearance. Confirm it with counsel rather than assuming in either direction, because parents both over-budget for clearances they do not need and get surprised when a specific customer raises foreign-ownership questions on unclassified work. Where mitigation does apply, your counsel owns the instrument and I build the operation that satisfies it.

What do you own, and what stays with our lawyers?

I stand up and run the compliant US operation: the floor, the operating model, the IT and OT build, the US-person data boundary, and the readiness evidence for the gate you are racing. Entity formation, FOCI mitigation, and site selection stay with your corporate counsel, your export-control counsel, and a site-selection advisor. I coordinate with them and own the operating outcome. That boundary is the reason the engagement works: you already have advisors for the legal instrument, and none of them is going to run your floor.

Sources

1. DFARS 225.003 Definitions, qualifying countries (acquisition.gov, current as of DFARS Change 5/7/2026)
   https://www.acquisition.gov/dfars/225.003-definitions.
2. ITAR 22 CFR 120.62, definition of U.S. person, including any entity incorporated to do business in the United States (eCFR)
   https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.62
3. ITAR 22 CFR 120.50, definition of export, including the deemed-export rule for releases to a foreign person in the United States (eCFR)
   https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.50
4. ITAR 22 CFR 122.1, registration requirements, exemptions, and purpose, including the requirement that a non-exporting manufacturer register (eCFR)
   https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-122/section-122.1
5. ITAR 22 CFR 126.5, Canadian exemptions, and its limits on foreign-parent access to controlled technical data (eCFR)
   https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126/section-126.5
6. Directorate of Defense Trade Controls, guidance on the Canadian exemption
   https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=KB0010128
7. CMMC Program rule, 32 CFR 170.3, applicability and the four-phase implementation schedule (eCFR)
   https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-A/section-170.3
8. CMMC Program rule, 32 CFR 170.14, the CMMC Model, where Level 2 requirements are identical to NIST SP 800-171 R2 (eCFR)
   https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.14
9. Cybersecurity Maturity Model Certification (CMMC) Program final rule, 89 FR 83214, published October 15, 2024, effective December 16, 2024 (Federal Register)
   https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program
10. DFARS: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), published September 10, 2025, effective November 10, 2025, the Phase 1 start date (Federal Register)
    https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
11. DoD CIO, About CMMC: the July 13, 2026 suspension of the Phase II requirements, the CMMC reform task force, the pause in Phase 1, and CMMC Level 2 as a self-assessment every three years against the 110 NIST SP 800-171 Revision 2 requirements with annual affirmation into SPRS, under DFARS clause 252.204-7012
    https://dodcio.defense.gov/CMMC/About/

12. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025)
https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements.

13. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024), including the FedRAMP Moderate equivalence requirement for external cloud providers and the 72-hour reporting clock
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

14. DCSA, Foreign Ownership, Control, or Influence (FOCI) and facility-clearance mitigation
https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/

15. Center for Development of Security Excellence, Foreign Ownership, Control, or Influence student guide
https://www.cdse.edu/Portals/124/Documents/student-guides/IS065-guide.pdf

16. DoD-CIO Standards Guide for Foreign Partners (2023), the controls overlay for foreign-owned US operations
https://dodcio.defense.gov/Portals/0/Documents/Library/StandardsGuideForeignPartners.pdf

17. American Rheinmetall achieves CMMC Level 2 certification for its US production facilities (2026-04-14)
https://www.rheinmetall.com/en/media/news-watch/news/2026/04/2026-04-14-american-rheinmetall-has-achieved-cmmc-level-2-certification-for-its-us-production-facilities

18. DFARS 225.870-1 General, contracting with Canadian contractors: Canada as part of the defense industrial base for production planning, and the Canadian Commercial Corporation's award and administration of DoD contracts with contractors located in Canada, subject to four named exceptions (acquisition.gov, current as of DFARS Change 5/7/2026)
https://www.acquisition.gov/dfars/225.870-1-general.

19. Canadian Commercial Corporation, prime contractor to the US Department of Defense
https://www.ccc.ca/en/services/prime-contractor-us/

20. Congressional Research Service R47599, AUKUS Pillar 2 (Advanced Capabilities)
https://www.congress.gov/crs-product/R47599

21. Dechert, CFIUS jurisdiction and greenfield investments
https://www.dechert.com/knowledge/onpoint/2023/12/what-dealmakers-should-know-about-congress--wish-list-for-cfius-.html

22. SelectUSA, US Department of Commerce International Trade Administration
https://www.trade.gov/selectusa

23. GEFRAN S.p.A., Italian sensor and automation multinational with a manufacturing plant in North Andover, Massachusetts
https://www.gefran.com/group/

24. One Thread, Two Flags: the US-person data boundary for a foreign-parented defense operation
/resources/one-thread-two-flags

25. The New England Landing Zone: where allied defense suppliers build their US operations
/resources/new-england-landing-zone

26. US market entry for allied defense manufacturers
    /us-market-entry
27. Standard Work 2.0, the four-pillar operating method
    /method
28. The three engagement models
    /engagements

NEXT STEP

Request the Market-Entry Conversation

garrettpartridge.com/booking