GARRETT PARTRIDGE

OPERATIONS ARCHITECT

COMPLIANCE

One Thread, Two Flags: The US-Person Data Boundary for a Foreign-Parented Defense Operation

How the US-person data boundary, the ITAR data border, and CMMC Level 2 are built into one auditable digital thread inside a foreign-owned US operation.

White Paper · Garrett Partridge · July 16, 2026

garrettpartridge.com · Brookline, NH

THE DIRECT ANSWER

Yes. A foreign-owned US subsidiary can hold ITAR-controlled technical data and reach CMMC Level 2. Neither regime asks who owns you. Both ask where the data sits and who can reach it. Under ITAR, your US subsidiary is a US person because it is incorporated in the United States, and your parent is a foreign person because it is not (22 CFR 120.62 and 120.63). Ownership does not change either answer. Releasing technical data to a foreign person inside the United States is an export, a deemed export (22 CFR 120.50(a)(2)), so your parent's engineers, IT administrators, and helpdesk are foreign recipients of your own subsidiary's data unless a license or exemption says otherwise. CMMC Level 2 then requires the NIST SP 800-171 controls on the systems that hold Controlled Unclassified Information, and proof that those controls actually run. What that takes in practice is one build, not three: a single US-person data boundary drawn around the controlled work, with the parent outside it, enforced by the same access control, segmentation, and logging an assessor scores. The org chart keeps two flags. The digital thread gets one.

Your parent company is a foreign person

The sentence that reorganizes this entire problem is short, and most parents hear it for the first time far too late. Under ITAR, your parent is a foreign person with respect to your US subsidiary's technical data. Not a partner with extra paperwork. A foreign person: the same category as any other company abroad that does not hold a license.

The regulation gets there on incorporation, not ownership. A US person includes any entity "incorporated to do business in the United States" (22 CFR 120.62). A foreign person includes any entity "not incorporated or organized to do business in the United States" (22 CFR 120.63). Your Delaware or Massachusetts entity is a US person. Your parent in Ottawa, Brescia, or Stuttgart is a foreign person. The parent owning 100 percent of the subsidiary moves neither one across the line. There is no family exception in the text, because the text never asks about the family.

Executives hear this as an insult to a corporate relationship they spent decades building. It is not. It is a statement about data, and only about data. The parent still owns the company, appoints the board, sets the strategy, and takes the profit. What the parent stops getting automatically is the drawing.

The same instinct shows up around allied status, so it is worth closing now. Every country I serve is a DFARS qualifying country under a reciprocal defense-procurement agreement with the Department of Defense (DFARS 225.003). That status is a procurement preference on end products and components. It does not waive ITAR, it does not waive CMMC, and it does not clear FOCI. Allied status gets your parts through the Buy American analysis. It does not get your parent through the data boundary.

ITAR does define foreign ownership and foreign control for its own purposes, at 22 CFR 120.65. Foreign ownership is more than 50 percent of the outstanding voting securities. Foreign control is the authority or ability to establish or direct general policies or day-to-day operations, and it is

presumed where foreign persons own 25 percent or more of the outstanding voting securities unless one US person controls an equal or larger percentage. Those definitions matter to what you tell the Directorate of Defense Trade Controls. They are ITAR's own, and they are not the Defense Counterintelligence and Security Agency's FOCI framework, which runs on separate rules. Keep the two apart, and let export counsel and a DCSA-facing specialist own their halves.

> **The test is incorporation, not ownership. Your US subsidiary is a US person because it is incorporated here. Your parent is a foreign person because it is not. Owning 100 percent of the subsidiary changes neither answer.**

What is actually inside the boundary

Before you can draw a boundary you have to know what it holds. Two populations of data are in play. They overlap heavily, and most shops misjudge both in exactly the same way: they wait for a marking.

ITAR technical data is information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of a defense article, including information in the form of blueprints, drawings, photographs, plans, instructions, or documentation (22 CFR 120.33(a)). Read that definition again and notice what is missing from it. There is no marking in it. Technical data is defined by what the information lets someone do, not by whether a stamp landed on the corner of the page. A CAM file nobody labeled is technical data if it is required to make the part.

Covered defense information runs on a parallel logic. Under DFARS 252.204-7012, it is unclassified controlled technical information or other CUI Registry information that requires safeguarding and is either marked or identified in the contract, or "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." That second prong needs no marking either.

So the instruction your staff has been living by, protect the marked material, is the wrong instruction. Two regimes, two definitions, and neither one waits for a sticker. Both attach on function and context, which is precisely why they cannot be delegated to whoever handles the stamp.

- Technical data is functional. If the information is required to design, make, test, repair, or modify the defense article, ITAR treats it as technical data, marked or not (22 CFR 120.33(a)).
- Covered defense information is contextual. Information used or stored in support of contract performance is covered defense information whether or not it arrived marked (DFARS 252.204-7012, definitions).
- The exclusions are real, and they are useful. ITAR technical data does not include general scientific, mathematical, or engineering principles commonly taught in universities, information in the public domain, or basic marketing information on function or purpose and general system descriptions of defense articles (22 CFR 120.33(b)). That carve-out is what lets your parent keep its reporting, and I come back to it at the end.
- The derived files are the ones that get you. The drawing is obvious and people handle it

carefully. The CAM file, the fixture print, the inspection program, and the process sheet derived from it are the ones that quietly land on an unowned share.

> **Your staff has been trained to look for a marking. ITAR technical data does not need one, and the second prong of covered defense information does not need one either. That gap is where a foreign-parented shop leaks first.**

The five group IT architectures that leak

This is the part that lands hardest in the room. The single biggest obstacle between an allied manufacturer and a DoD contract is usually not the regulation. It is the group IT architecture the parent spent fifteen years standardizing, and is rightly proud of.

Under 22 CFR 120.56(a)(3), technical data is released through the use of access information to cause or enable a foreign person to access, view, or possess unencrypted technical data. Read the verb. Enable. The clause is written on capability, not on intent, and not on whether anyone opened the file. Under 22 CFR 120.56(b), authorization for a release is required in order to provide that access information to a foreign person in the first place. So the question an export lawyer and an assessor both ask is not whether the parent looked. It is whether the parent could be enabled to reach it.

Five patterns account for most of what I find on a first walk:

- The shared ERP or PLM instance. One group tenant, one part master, one document vault, and a parent-side engineering group with read access across the whole thing. The efficiency that made it worth building is exactly the problem.
- The group file share. A global share or tenant where the US site is a folder. Controlled drawings land there because that is where drawings have always landed, and every group user with a path to that folder is a reachability question.
- The offshore or parent-country helpdesk. The service desk that supports every site, holds administrative rights on every endpoint, and can take a remote session on a workstation with a drawing open. The support is genuinely good. That is why it was centralized.
- Parent-hosted identity and network. The parent's domain, the parent's VPN, the parent's domain administrators. An administrator who can reset any password can enable access to anything that password protects. That is 22 CFR 120.56(a)(3) written as a job description.
- Group backup and disaster recovery. Replication to the parent's datacenter, with the parent's storage team holding the restore keys. Nobody thinks of backup as a data path. It is the most complete data path in the building.

> The question is never whether the parent looked at the drawing. Under 22 CFR 120.56(a)(3), the question is whether the parent could be enabled to reach it. Capability is the trigger, and a domain administrator's capability is total by design.

Encryption moves the bits. It does not move the authority.

The first idea every capable CTO brings to this problem is encryption, and the instinct is right. ITAR gives encryption a real carve-out. That carve-out is both more useful and more narrow than nearly everyone believes, and the gap between those two readings is where programs get expensive.

Here is what it grants. Under 22 CFR 120.54(a)(5), sending, taking, or storing technical data is not an export when the data is unclassified, secured using end-to-end encryption, and secured using cryptographic modules compliant with FIPS 140-2 or its successors, or by other cryptographic means providing security strength at least comparable to the minimum 128 bits achieved by AES-128, and not intentionally sent to a person in or stored in a country proscribed under 22 CFR 126.1, and not sent from one. The rule even settles the routing anxiety directly: data in transit via the internet is not deemed to be stored in a country it transits. And 22 CFR 120.54(c) states plainly that the ability to access technical data in encrypted form meeting those criteria does not constitute a release or an export.

Now read the definition the carve-out runs on. For this purpose, end-to-end encryption requires that the data not be in unencrypted form between the originator and the intended recipient, and that "the means of decryption are not provided to any third party" (22 CFR 120.54(b)(1)). The intended recipient has to be the originator, a US person in the United States, or a person otherwise authorized to receive the technical data (22 CFR 120.54(b)(2)).

That is where it collapses for most group architectures. Access information is defined at 22 CFR 120.55 as information allowing access to encrypted technical data in unencrypted form, and the regulation names the examples itself: decryption keys, network access codes, and passwords. Provide those to a foreign person and 22 CFR 120.56(b) requires authorization to do it. Use them to enable a foreign person to reach unencrypted data and you are inside 22 CFR 120.56(a)(3), a release. And 22 CFR 120.50(a)(6) makes the release of previously encrypted technical data an export in its own right.

So the architecture falls out of the text, and it is the thesis of this paper. The ciphertext can cross the group's infrastructure. The keys cannot cross to the parent. Your parent can hold the storage, carry the traffic, own the pipe, and run the replication, so long as what it holds stays unreadable to it and the means of decryption stay inside the US-person boundary. That single asymmetry is what lets one company keep one IT relationship and two flags.

Two cautions, and I mean both of them. The conditions in 22 CFR 120.54(a)(5), plus the definition in (b), are conjunctive: they all have to hold, on your actual facts, at the same time. And whether your specific architecture qualifies is a legal determination your export counsel makes, not one an operations architect makes for you. My job is to build the environment so that determination is clean, documented, and easy to answer yes to. The determination itself stays with counsel, and I

say that in the first meeting rather than the last.

> **The bits can cross. The keys cannot. A parent holding only ciphertext, with the means of decryption never provided to it, is holding storage. A parent holding the key is holding technical data.**

CMMC does not draw the line. It proves the line is real.

Most foreign-parented shops run ITAR and CMMC as two projects, with two vendors and two budgets, and often a third for the network build. They are one build. Understanding why saves the six months these programs usually lose.

NIST SP 800-171 is citizenship-blind. Its access controls ask whether a user is authorized. They do not ask what passport the user holds. That is not a gap in the standard, it is a division of labor. ITAR is the regime that decides who can be authorized for export-controlled technical data. NIST SP 800-171 is the machinery that enforces the decision, logs it, and generates the evidence. CMMC Level 2 is the Department of Defense checking that the machinery is real.

Which fixes the sequence. ITAR draws the boundary. The 800-171 controls hold it. The assessor scores it. Build them in that order and each one feeds the next: the access matrix you write for the export question becomes the access control the assessor tests. Build them as three parallel vendor conversations and you get three answers that contradict each other at the gate.

One definition inside DFARS 252.204-7012 ends the most common plan I hear, which is that the group IT organization will simply run the US site the way it runs every other site. A covered contractor information system is defined as "an unclassified information system that is owned, or operated by or for, a contractor" and that processes, stores, or transmits covered defense information. Operated by or for. If your parent's IT department operates your US systems, those systems are covered contractor information systems, and the parent's environment is not outside your assessment. It is inside it. Handing the work to the group does not move the obligation offshore. It pulls the group into scope.

The clause carries the rest of the shape you have to plan for:

- Implement NIST SP 800-171 on covered contractor information systems, in the revision in effect at the time the solicitation is issued, or as authorized by the Contracting Officer (DFARS 252.204-7012(b)(2)(i)). The revision is pinned to the solicitation, so scope the control set against the contract in front of you rather than against a vendor's slide.
- An external cloud service provider that stores, processes, or transmits covered defense information has to meet security requirements equivalent to the FedRAMP Moderate baseline, and comply with the clause's cyber incident reporting, malicious software, media preservation, forensic access, and damage assessment paragraphs (DFARS 252.204-7012(b)(2)(ii)(D)). If the group's hosting is that provider, the group is signing up to all of it.
- Report a cyber incident within 72 hours of discovery. The clause defines "rapidly report" as exactly that. A parent-run helpdesk five time zones away is now inside your 72-hour clock, which is a staffing question before it is a compliance question.
- The clause flows down to subcontracts without alteration, except to identify the parties

(DFARS 252.204-7012(m)). Group affiliates are not exempt from it because they share your logo.

- CMMC Level 2 means the 110 security requirements of NIST SP 800-171, and as of July 2026 it is reached by a self-assessment every three years with an annual affirmation into SPRS. On July 13, 2026 the Department suspended the Phase II third-party certification requirement and opened a reform review. The clause above did not move, so a new US operation still cannot treat the boundary as a year-two project. What changed is who states that the controls run. It is now you.

> **Operated by or for.** If the parent's IT department runs your systems, the parent's systems are inside your CMMC assessment. Centralizing with the group does not move the obligation offshore. It pulls the group inside the boundary.

The boundary does not stop at the office

Everything so far is easy to picture as an office problem. File shares, mailboxes, an ERP, a helpdesk. That framing is precisely how foreign-parented shops fail, because the controlled data does its most dangerous traveling on the floor.

The moment a drawing leaves the ERP and becomes a work instruction at the machine, technical data has crossed from a system you treat as protected into a system you have historically treated as a machine rather than a computer. The CAM file on a shared floor PC. The program sitting on the controller. The historian logging process data tied to a controlled part, then syncing to a server the whole office can reach. For a domestic shop, that crossing is already the most overlooked control point in the building. For a foreign-parented shop, every one of those crossings carries a second question stacked on top of the first: not only whether this is controlled, but who at the group can reach the system it landed on.

The example that makes this concrete is not a villain. It is your best automation engineer. A line goes down in Nashua at 2 a.m. The parent's controls engineer in Turin commissioned that exact cell four times and can have it running in twenty minutes over a remote session. He is a foreign person. The controller holds a program derived from controlled technical data. That remote session is the entire regulation in one screen share, and the supervisor on shift is going to make that call at 2 a.m. unless the architecture already made it for him.

So the boundary gets designed into the floor rather than drawn around it. Segment the OT network so a reachable office endpoint is not a path to a controller. Route the necessary hand-offs through a controlled, logged conduit instead of a USB drive. Decide in advance, in writing, which cells hold controlled programs and who may reach them, so the 2 a.m. decision is a lookup instead of a judgment call. And where the group's engineering support genuinely is the right answer, get it authorized properly through counsel while the line is still running, rather than discovering the question during an incident.

This is why I treat the data border and the operating model as one design problem rather than two. The same converged thread that gives an assessor a single auditable path from the contract to the cut is the thread that gives the P&L an honest view of what the floor is actually doing. Built once, it is the auditor's evidence and the owner's instrument panel. Built twice, it is two systems

that disagree.

> **The regulation does not care that it was 2 a.m. and the line was down. Decide who may reach a controller holding a controlled program before the night the line goes down, and it stops being the shift supervisor's decision to make.**

The org chart keeps two flags

Every parent hears the US-person data boundary as a wall between itself and the company it owns. That reading kills more of these projects than any control does, and it is wrong. Built properly, the parent loses almost nothing it actually needs.

Go back to the definition. ITAR technical data is information required to design, make, test, repair, or modify a defense article, and 22 CFR 120.33(b) expressly excludes basic marketing information on function or purpose and general system descriptions. Consolidated financials are not technical data. Order intake, backlog, on-time delivery, scrap rate, throughput, headcount, capex, quality metrics, and the SQDIP board are not technical data. Almost nothing a parent's board actually reviews on a Tuesday is technical data.

So the design task is precise, and it is an operating task rather than a legal one: give the parent every number it is entitled to, and none of the drawings it is not. In practice the reporting layer is built to cross the boundary and the engineering layer is built not to. That distinction is the whole architecture, and it is why this gets decided at design time, when it costs a conversation, instead of at assessment time, when it costs a re-platform.

- Crosses the boundary by design: consolidated financials, order intake and backlog, on-time delivery, scrap and yield, throughput, headcount, capex, and the SQDIP cadence. The parent's board keeps its Tuesday review.
- Stays inside the boundary: drawings, specifications, CAM and inspection programs, process sheets, and every derived file required to make, test, or repair the article (22 CFR 120.33(a)).
- Stays inside the boundary: the keys. Decryption keys, network access codes, and passwords are access information (22 CFR 120.55), and providing them to a foreign person requires authorization (22 CFR 120.56(b)).
- Named, and written down: a US-person system administrator for the enclave, a named US-person owner of the access decision, and a technical data access matrix that names, by role and citizenship, who may reach controlled data and who may not. A prime's auditor and a DDTC reviewer both ask for that matrix. A verbal understanding is not an artifact.
- Separate question, separate schedule: FOCI. FOCI mitigation is what DCSA requires when a foreign-owned company needs eligibility to access classified information, negotiated through your cleared-facility counsel. Most sub-tier defense manufacturing is unclassified CUI and ITAR-controlled work that never needs a facility clearance at all. That work still needs this data boundary on day one. FOCI is conditional on the class of work you chase. The data boundary is not conditional at all.

> **The parent keeps the company, the governance, and every number its board reviews. The subsidiary keeps the drawings. That is not a wall between a parent and its investment. It is the only architecture under which that investment wins the contract.**

What I build, and what stays with counsel

I am the operations partner, and I am precise about the edge of that. 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, ITAR and DDTC registration, FOCI mitigation, license and exemption determinations, and CFIUS questions stay with your corporate counsel and your export-control counsel. I coordinate with them and own the operating outcome.

That line is not modesty, it is the reason the build holds. Whether a specific architecture qualifies for the 22 CFR 120.54 carve-out, whether a specific transfer needs a license, whether your ownership structure triggers a DDTC notification: those are legal determinations with legal consequences. An operations architect who answers them for you is selling you a liability with a confident voice. What I do is build the operation so those determinations are clean, documented, and easy, and so the evidence exists before anyone asks for it.

This build is not theoretical and it is not rare. In April 2026, American Rheinmetall achieved CMMC Level 2 certification across its US production facilities: a German-parented US operation holding the posture, on the public record. I have been the foreign parent's operator in the US myself, running an Italian sensor multinational's North America operations, and I am standing up US defense manufacturing operations for a Canadian-parent subsidiary now. The path exists and people are walking it. What is scarce is the operator who walks it with you. Six tiers of firms will help a foreign manufacturer enter the US market, from FOCI counsel to Big-4 structuring to site selection to CMMC IT vendors, and every one of them hands you a document, a building, or a certificate. The DoD Chief Information Officer's Standards Guide for Foreign Partners is the closest thing to an official synthesis, and it is a controls overlay rather than an operator's sequence. Someone still has to stand up and run the operation. That layer is the work, and it is the one I own.

The bottom line is the title. Your parent is a foreign person with respect to your US subsidiary's technical data, so the drawings, the derived files, and the keys stay inside a US-person boundary while the ciphertext, the financials, and the governance cross it freely. ITAR draws that boundary, NIST SP 800-171 holds it, and CMMC Level 2 proves it holds. Build the three as one thread and the assessor finds the controls already running, because they are how the work gets done. Build them as three vendor conversations and you learn which one was wrong at the gate, with the contract on the table. One thread. Two flags.

FREQUENTLY ASKED

Is our parent really a foreign person if it owns 100 percent of us?

Yes. Under ITAR the test for an entity is incorporation, not ownership. A US person includes any entity incorporated to do business in the United States (22 CFR 120.62), and a foreign person includes any entity not incorporated or organized to do business in the United States (22 CFR 120.63). Your US subsidiary is a US person. Your parent, incorporated abroad, is a foreign person. Owning all of the subsidiary moves neither across the line, because the definitions never ask about ownership. ITAR does define foreign ownership and foreign control separately at 22 CFR 120.65, and those definitions matter to what you report to the Directorate of Defense Trade Controls. They do not create a family exception to the data rules.

Can our US site run on the parent company's ERP?

Usually not without a boundary. If your US operation holds controlled technical data, that data stays inside a US-person data boundary, so a shared instance that gives parent-side users a path to drawings or specifications is a release question under 22 CFR 120.56(a)(3), which turns on whether a foreign person can be enabled to reach unencrypted technical data. Sometimes the answer is a segregated instance, sometimes a separate system, sometimes a controlled interface that passes planning and financial data upward while the engineering vault stays inside the boundary. The architecture decision is part of the build, and it gets made against your actual data flows rather than a template.

Does encrypting everything solve the problem?

Encryption solves the transport problem, not the authority problem. ITAR provides a real carve-out at 22 CFR 120.54(a)(5) for sending, taking, or storing unclassified technical data under end-to-end encryption meeting FIPS 140-2 or comparable strength, and 22 CFR 120.54(c) confirms that the ability to access properly encrypted data is not a release or an export. But the carve-out is defined to require that the means of decryption are not provided to any third party (22 CFR 120.54(b)(1)), and decryption keys, network access codes, and passwords are access information under 22 CFR 120.55. Provide those to a foreign person and you are in 22 CFR 120.56, a release, and an export under 22 CFR 120.50(a)(6). So the parent can hold ciphertext. The parent cannot hold the key. Whether your specific setup satisfies every condition of the carve-out is a determination for your export counsel.

Can our parent's IT department administer our US systems?

Not without pulling the parent into your assessment, and not without answering the ITAR question first. DFARS 252.204-7012 defines a covered contractor information system as one owned, or operated by or for, a contractor that processes, stores, or transmits covered defense information. If the parent operates your systems, those systems are covered contractor information systems and the parent's environment sits inside your CMMC scope. Separately, an administrator who can reset a password can enable access to what that password protects, which is the release standard at 22 CFR 120.56(a)(3). The workable answer is usually US-person administration of the enclave, with the group keeping everything outside it.

Does the Canadian exemption let our Canadian parent reach our US subsidiary's technical data?

No, and this is the most common misreading in the Canada lane. The exemption at 22 CFR 126.5 authorizes license-free export of unclassified US Munitions List articles and services from the United States to a Canadian-registered person or Canadian government end use, with exclusions, and with prior approval from the Directorate of Defense Trade Controls required for reexport or retransfer. It authorizes an export, in a direction, under conditions. It does not grant a Canadian parent a standing right to reach ITAR technical data held by its US subsidiary. That misreading is exactly why the US-person data boundary gets built. Your export counsel confirms what the exemption covers on your facts.

Do we need FOCI mitigation before we can hold ITAR technical data?

Those are two questions on two different schedules. FOCI mitigation is what the Defense Counterintelligence and Security Agency requires when a foreign-owned company needs eligibility to access classified information, negotiated with DCSA through your cleared-facility counsel. Most sub-tier defense manufacturing is unclassified CUI and ITAR-controlled work that never needs a facility clearance, so FOCI mitigation may never enter your scope at all. The US-person data boundary works differently. If you hold controlled technical data, it applies from the first day you hold it. Knowing which class of work you are chasing is what decides whether FOCI is even in the conversation.

Does CMMC require US citizens?

CMMC does not decide that question. The NIST SP 800-171 access controls ask whether a user is authorized, not what passport the user holds. ITAR is the regime that decides who can be authorized for export-controlled technical data, and a foreign person needs a license or an exemption. The two compose rather than compete: ITAR draws the line, the 800-171 controls enforce and log it, and the CMMC Level 2 assessment scores whether it is real. That is also why building them as one program works, and why building them as three vendor conversations produces three answers that disagree at the gate.

Sources

1. ITAR 22 CFR 120.63, foreign person (eCFR). The incorporation test that makes a foreign parent a foreign person to its own US subsidiary
   https://www.ecfr.gov/current/title-22/section-120.63
2. ITAR 22 CFR 120.62, U.S. person (eCFR). Any entity incorporated to do business in the United States
   https://www.ecfr.gov/current/title-22/section-120.62
3. ITAR 22 CFR 120.50, export, including the deemed export of technical data to a foreign person in the United States at (a)(2) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.50
4. ITAR 22 CFR 120.33, technical data. The functional definition that attaches without a marking (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.33
5. ITAR 22 CFR 120.54, activities that are not exports, including the end-to-end encryption carve-out at (a)(5) and its definition at (b) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.54
6. ITAR 22 CFR 120.55, access information. Decryption keys, network access codes, and passwords (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.55
7. ITAR 22 CFR 120.56, release. Using access information to enable a foreign person to reach unencrypted technical data (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.56
8. ITAR 22 CFR 120.65, foreign ownership and foreign control, as ITAR defines them for its own purposes (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.65
9. ITAR 22 CFR 126.5, Canadian exemptions (eCFR), and its limits on foreign-parent access to controlled technical data
   https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126/section-126.5
10. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (acquisition.gov, clause dated May 2024, current as of DFARS Change 5/7/2026)
    https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
11. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, at the location DFARS 252.204-7012(b)(2)(i) cites
    https://csrc.nist.gov/publications/sp800
12. DoD CIO, About CMMC: the July 13, 2026 suspension of the Phase II requirements, 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/

13. DFARS 225.003 Definitions, qualifying countries (acquisition.gov, current as of DFARS Change 5/7/2026)
https://www.acquisition.gov/dfars/225.003-definitions.

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. 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

16. 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

17. Standard Work 2.0, the four-pillar operating method, and the Sovereign Tier pillar where the data borders are set
/method

18. The US Market-Entry Playbook for Allied Defense Manufacturers, the full operational stand-up sequence this paper sits inside
/resources/us-market-entry-playbook

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

20. IT/OT Convergence for Defense Manufacturers: why MES, ERP, and SCADA are three compliance liabilities until they are one
/blog/it-ot-convergence-defense-manufacturers

21. Foreign Manufacturer Onshoring Playbook: standing up US defense manufacturing operations in 90 days
/blog/foreign-manufacturer-onshoring-90-day-playbook

NEXT STEP

Request a Strategic Conversation

garrettpartridge.com/booking