CONFORMITÀ

Un solo filo, due bandiere: il confine dei dati riservato ai US-person per un'operazione di difesa a controllo estero

Come il confine dei dati riservato ai US-person, il confine dei dati ITAR e la CMMC Level 2 vengono costruiti in un unico filo digitale verificabile dentro un'operazione statunitense a controllo estero.

White paper · Garrett Partridge · 16 luglio 2026

garrettpartridge.com · Brookline, NH

LA RISPOSTA DIRETTA

Sì. Una filiale statunitense a controllo estero può detenere dati tecnici soggetti a controllo ITAR e raggiungere la CMMC Level 2. Nessuno dei due regimi chiede chi La possiede. Entrambi chiedono dove risiedono i dati e chi può raggiungerli. Ai sensi dell'ITAR, la Sua filiale statunitense è una US person perché è costituita negli Stati Uniti, e la Sua casa madre è una foreign person perché non lo è (22 CFR 120.62 e 120.63). La proprietà non cambia nessuna delle due risposte. Rilasciare dati tecnici a una foreign person all'interno degli Stati Uniti è un'esportazione, un deemed export (22 CFR 120.50(a)(2)), quindi gli ingegneri, gli amministratori IT e il servizio di assistenza della Sua casa madre sono destinatari esteri dei dati della Sua stessa filiale, a meno che una licenza o un'esenzione non dispongano altrimenti. La CMMC Level 2 richiede poi i controlli del NIST SP 800-171 sui sistemi che detengono Controlled Unclassified Information, e la prova che quei controlli siano davvero in funzione. Ciò che serve in pratica è un solo cantiere, non tre: un unico confine dei dati riservato ai US-person tracciato attorno al lavoro controllato, con la casa madre al di fuori, imposto dagli stessi controlli di accesso, dalla stessa segmentazione e dalla stessa registrazione dei log che un valutatore misura. L'organigramma conserva due bandiere. Il filo digitale ne prende una.

La Sua casa madre è una foreign person

La frase che riorganizza tutto questo problema è breve, e la maggior parte delle case madri la sente per la prima volta troppo tardi. Ai sensi dell'ITAR (la normativa statunitense sul controllo delle esportazioni di materiale d'armamento), la Sua casa madre è una foreign person (una persona straniera ai sensi dell'ITAR) rispetto ai dati tecnici della Sua filiale statunitense. Non un partner con qualche adempimento in più. Una foreign person: la stessa categoria di qualunque altra società all'estero che non sia titolare di una licenza.

La norma ci arriva attraverso la costituzione societaria, non attraverso la proprietà. Una US person (una persona statunitense ai sensi dell'ITAR) comprende qualunque entità "incorporated to do business in the United States", costituita per operare negli Stati Uniti (22 CFR 120.62). Una foreign person comprende qualunque entità "not incorporated or organized to do business in the United States", non costituita né organizzata per operare negli Stati Uniti (22 CFR 120.63). La Sua entità del Delaware o del Massachusetts è una US person. La Sua casa madre a Ottawa, a Brescia o a Stoccarda è una foreign person. Il fatto che la casa madre possieda il 100 per cento della filiale non sposta né l'una né l'altra oltre quella linea. Nel testo non esiste alcuna eccezione familiare, perché il testo non chiede mai della famiglia.

I dirigenti lo percepiscono come un affronto a un rapporto societario che hanno impiegato decenni a costruire. Non lo è. È un'affermazione sui dati, e soltanto sui dati. La casa madre continua a possedere la società, a nominare il consiglio, a fissare la strategia e a incassare l'utile. Ciò che la casa madre smette di ricevere automaticamente è il disegno.

Lo stesso istinto riaffiora attorno allo status di alleato, quindi conviene chiuderlo subito. Ogni paese che servo è un paese qualificato ai sensi del DFARS (il supplemento alla normativa federale statunitense sugli appalti della difesa) nell'ambito di un accordo reciproco sugli appalti della

difesa con il Dipartimento della Difesa (DFARS 225.003). Quello status è una preferenza negli appalti sui prodotti finiti e sui componenti. Non esonera dall'ITAR, non esonera dalla CMMC (il livello di maturità in cybersicurezza richiesto dalla difesa statunitense), e non risolve la questione FOCI (proprietà, controllo o influenza stranieri). Lo status di alleato fa passare i Suoi pezzi attraverso l'analisi Buy American. Non fa passare la Sua casa madre attraverso il confine dei dati.

L'ITAR definisce effettivamente la proprietà estera e il controllo estero per i propri fini, al 22 CFR 120.65. La proprietà estera è oltre il 50 per cento dei titoli con diritto di voto in circolazione. Il controllo estero è l'autorità o la capacità di stabilire o dirigere le politiche generali o le operazioni quotidiane, ed è presunto quando delle foreign person possiedono il 25 per cento o più dei titoli con diritto di voto in circolazione, a meno che una singola US person non ne controlli una percentuale uguale o superiore. Quelle definizioni contano per ciò che dichiara alla Directorate of Defense Trade Controls. Sono definizioni proprie dell'ITAR, e non sono il quadro FOCI della Defense Counterintelligence and Security Agency, che poggia su regole distinte. Tenga separate le due cose, e lasci che il consulente in materia di controllo delle esportazioni e uno specialista nel rapporto con la DCSA rispondano ciascuno della propria metà.

> **Il criterio è la costituzione societaria, non la proprietà. La Sua filiale statunitense è una US person perché è costituita qui. La Sua casa madre è una foreign person perché non lo è. Possedere il 100 per cento della filiale non cambia nessuna delle due risposte.**

Che cosa c'è davvero dentro il confine

Prima di poter tracciare un confine deve sapere che cosa contiene. In gioco ci sono due popolazioni di dati. Si sovrappongono ampiamente, e la maggior parte delle officine le giudica male entrambe esattamente nello stesso modo: aspetta una marcatura.

I dati tecnici ai sensi dell'ITAR sono le informazioni necessarie alla progettazione, allo sviluppo, alla produzione, alla fabbricazione, all'assemblaggio, al funzionamento, alla riparazione, al collaudo, alla manutenzione o alla modifica di un defense article (un articolo della difesa ai sensi dell'ITAR), comprese le informazioni sotto forma di schemi costruttivi, disegni, fotografie, piani, istruzioni o documentazione (22 CFR 120.33(a)). Rilegga quella definizione e noti che cosa vi manca. Non c'è alcuna marcatura. I dati tecnici sono definiti da ciò che l'informazione permette di fare, non dal fatto che un timbro sia finito sull'angolo della pagina. Un file CAM che nessuno ha etichettato è un dato tecnico se è necessario a fabbricare il pezzo.

Le covered defense information (le informazioni di difesa soggette alla clausola) seguono una logica parallela. Ai sensi del DFARS 252.204-7012 sono informazioni tecniche controllate non classificate, o altre informazioni del CUI Registry, che richiedono tutela e che sono marcate o individuate nel contratto, oppure "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract", cioè raccolte, sviluppate, ricevute, trasmesse, utilizzate o conservate dal contraente o per suo conto a supporto dell'esecuzione del contratto. Nemmeno quel secondo criterio richiede una marcatura.

Quindi l'istruzione con cui il Suo personale ha vissuto finora, proteggere il materiale marcato, è l'istruzione sbagliata. Due regimi, due definizioni, e nessuno dei due aspetta un'etichetta. Entrambi si attivano sulla funzione e sul contesto, ed è esattamente per questo che non possono

essere delegati a chi si occupa del timbro.

- I dati tecnici sono funzionali. Se l'informazione è necessaria a progettare, fabbricare, collaudare, riparare o modificare il defense article, l'ITAR la tratta come dato tecnico, marcata o no (22 CFR 120.33(a)).
- Le covered defense information sono contestuali. Un'informazione utilizzata o conservata a supporto dell'esecuzione del contratto è covered defense information a prescindere dal fatto che sia arrivata marcata (DFARS 252.204-7012, definizioni).
- Le esclusioni sono reali e sono utili. I dati tecnici ai sensi dell'ITAR non comprendono i principi generali scientifici, matematici o ingegneristici comunemente insegnati nelle università, le informazioni di pubblico dominio, né le informazioni di marketing di base su funzione o finalità e le descrizioni generali di sistema dei defense article (22 CFR 120.33(b)). È quella deroga a permettere alla Sua casa madre di conservare la propria reportistica, e ci torno alla fine.
- Sono i file derivati a metterLa nei guai. Il disegno è evidente e le persone lo maneggiano con cura. Il file CAM, il disegno dell'attrezzatura, il programma di collaudo e il foglio di processo che ne derivano sono quelli che finiscono silenziosamente su una cartella condivisa senza padrone.

> **Il Suo personale è stato addestrato a cercare una marcatura. I dati tecnici ai sensi dell'ITAR non ne hanno bisogno, e nemmeno il secondo criterio delle covered defense information ne ha bisogno. È in quella lacuna che un'officina a controllo estero perde per prima.**

Le cinque architetture IT di gruppo che perdono

È la parte che colpisce più duro in una sala riunioni. Il singolo ostacolo più grande tra un produttore alleato e un contratto del DoD (Dipartimento della Difesa degli Stati Uniti) di solito non è la norma. È l'architettura IT di gruppo che la casa madre ha impiegato quindici anni a standardizzare, e di cui va giustamente fiera.

Ai sensi del 22 CFR 120.56(a)(3), i dati tecnici sono rilasciati mediante l'uso di access information (le informazioni di accesso) per far sì che una foreign person acceda a dati tecnici non cifrati, li visualizzi o li detenga, oppure per metterla in condizione di farlo. Legga il verbo. Mettere in condizione. La clausola è scritta sulla capacità, non sull'intenzione, e non sul fatto che qualcuno abbia aperto il file. Ai sensi del 22 CFR 120.56(b), un'autorizzazione al rilascio è richiesta già solo per fornire quelle access information a una foreign person. Quindi la domanda che pongono sia un avvocato esperto di esportazioni sia un valutatore non è se la casa madre abbia guardato. È se la casa madre potesse essere messa in condizione di raggiungerli.

Cinque schemi spiegano la maggior parte di ciò che trovo a una prima ricognizione:

- L'istanza ERP (il sistema gestionale aziendale) o PLM condivisa. Un unico tenant di gruppo, un'unica anagrafica articoli, un unico archivio documentale, e un gruppo di ingegneria lato casa madre con accesso in lettura su tutto quanto. L'efficienza che ha reso quel sistema degno di essere costruito è esattamente il problema.
- La cartella condivisa di gruppo. Una condivisione o un tenant globale in cui il sito statunitense è una cartella. I disegni controllati finiscono lì perché è lì che i disegni sono sempre finiti, e ogni

utente del gruppo che ha un percorso verso quella cartella è una questione di raggiungibilità.

- Il servizio di assistenza delocalizzato o situato nel paese della casa madre. Il service desk che supporta ogni sito, detiene i diritti amministrativi su ogni endpoint, e può aprire una sessione remota su una postazione con un disegno aperto. L'assistenza è davvero buona. È per questo che è stata centralizzata.
- Identità e rete ospitate dalla casa madre. Il dominio della casa madre, la VPN della casa madre, gli amministratori di dominio della casa madre. Un amministratore che può reimpostare qualunque password può mettere qualcuno in condizione di accedere a tutto ciò che quella password protegge. È il 22 CFR 120.56(a)(3) scritto sotto forma di mansionario.
- Backup e disaster recovery di gruppo. La replica verso il datacenter della casa madre, con il team storage della casa madre che detiene le chiavi di ripristino. Nessuno pensa al backup come a un percorso dei dati. È il percorso dei dati più completo dell'edificio.

> **La domanda non è mai se la casa madre abbia guardato il disegno. Ai sensi del 22 CFR 120.56(a)(3), la domanda è se la casa madre potesse essere messa in condizione di raggiungerlo. È la capacità a far scattare la norma, e la capacità di un amministratore di dominio è totale per progettazione.**

La cifratura sposta i bit. Non sposta l'autorità.

La prima idea che ogni CTO capace porta a questo problema è la cifratura, e l'istinto è giusto. L'ITAR concede alla cifratura una deroga reale. Quella deroga è insieme più utile e più stretta di quanto quasi tutti credano, ed è nello scarto tra queste due letture che i programmi diventano costosi.

Ecco che cosa concede. Ai sensi del 22 CFR 120.54(a)(5), inviare, portare con sé o conservare dati tecnici non è un'esportazione quando i dati sono non classificati, protetti mediante cifratura end-to-end, e protetti mediante moduli crittografici conformi al FIPS 140-2 o ai suoi successori, oppure con altri mezzi crittografici che offrano una robustezza almeno comparabile ai 128 bit minimi raggiunti da AES-128, e quando non sono inviati intenzionalmente a una persona che si trova in un paese proscritto ai sensi del 22 CFR 126.1 né vi sono conservati, né sono inviati da uno di essi. La norma risolve perfino direttamente l'ansia sull'instradamento: i dati in transito su internet non si considerano conservati in un paese che attraversano. E il 22 CFR 120.54(c) afferma chiaramente che la possibilità di accedere a dati tecnici in forma cifrata che soddisfino quei criteri non costituisce né un rilascio né un'esportazione.

Ora legga la definizione su cui poggia la deroga. A questo fine, la cifratura end-to-end richiede che i dati non siano in forma non cifrata tra il mittente originario e il destinatario previsto, e che "the means of decryption are not provided to any third party", cioè che i mezzi di decifratura non siano forniti ad alcun terzo (22 CFR 120.54(b)(1)). Il destinatario previsto deve essere il mittente originario, una US person negli Stati Uniti, o una persona altrimenti autorizzata a ricevere quei dati tecnici (22 CFR 120.54(b)(2)).

Ed è qui che crolla per la maggior parte delle architetture di gruppo. Le access information sono definite al 22 CFR 120.55 come le informazioni che consentono di accedere in forma non cifrata a

dati tecnici cifrati, e la norma ne nomina essa stessa gli esempi: chiavi di decifratura, codici di accesso alla rete e password. Le fornisca a una foreign person e il 22 CFR 120.56(b) richiede un'autorizzazione per farlo. Le usi per mettere una foreign person in condizione di raggiungere dati non cifrati e si trova dentro il 22 CFR 120.56(a)(3), un rilascio. E il 22 CFR 120.50(a)(6) rende il rilascio di dati tecnici precedentemente cifrati un'esportazione a pieno titolo.

Così l'architettura discende dal testo, ed è la tesi di questo documento. Il testo cifrato può attraversare l'infrastruttura del gruppo. Le chiavi non possono passare alla casa madre. La Sua casa madre può detenere lo storage, trasportare il traffico, possedere il collegamento e gestire la replica, purché ciò che detiene resti per lei illeggibile e i mezzi di decifratura restino dentro il confine riservato ai US-person. È questa singola asimmetria a permettere a una società di conservare un solo rapporto IT e due bandiere.

Due avvertenze, ed entrambe le intendo sul serio. Le condizioni del 22 CFR 120.54(a)(5), più la definizione della lettera (b), sono cumulative: devono valere tutte insieme, sui Suoi fatti concreti, nello stesso momento. E se la Sua specifica architettura rientri o meno nella deroga è una valutazione giuridica che spetta al Suo consulente in materia di controllo delle esportazioni, non a un architetto delle operazioni. Il mio compito è costruire l'ambiente affinché quella valutazione sia netta, documentata e facile da chiudere con un sì. La valutazione in sé resta al consulente legale, e lo dico al primo incontro, non all'ultimo.

> **I bit possono attraversare. Le chiavi no. Una casa madre che detiene soltanto testo cifrato, e a cui i mezzi di decifratura non sono mai stati forniti, sta detenendo dello storage. Una casa madre che detiene la chiave sta detenendo dati tecnici.**

La CMMC non traccia la linea. Dimostra che la linea è reale.

La maggior parte delle officine a controllo estero gestisce ITAR e CMMC come due progetti, con due fornitori e due budget, e spesso un terzo per la costruzione della rete. Sono un unico cantiere. Capire il perché fa risparmiare i sei mesi che questi programmi di solito perdono.

Il NIST SP 800-171 (lo standard statunitense per la protezione delle informazioni controllate non classificate) è cieco rispetto alla cittadinanza. I suoi controlli di accesso chiedono se un utente sia autorizzato. Non chiedono quale passaporto quell'utente abbia. Non è una lacuna dello standard, è una divisione del lavoro. L'ITAR è il regime che decide chi può essere autorizzato ad accedere a dati tecnici soggetti a controllo delle esportazioni. Il NIST SP 800-171 è il meccanismo che impone quella decisione, la registra e produce le prove. La CMMC Level 2 è il Dipartimento della Difesa che verifica che quel meccanismo sia reale.

Il che fissa la sequenza. L'ITAR traccia il confine. I controlli 800-171 lo tengono. Il valutatore lo misura. Li costruisca in quest'ordine e ciascuno alimenta il successivo: la matrice degli accessi che redige per la questione delle esportazioni diventa il controllo di accesso che il valutatore mette alla prova. Li costruisca come tre trattative parallele con tre fornitori e ottiene tre risposte che si contraddicono al varco.

Una definizione contenuta nel DFARS 252.204-7012 chiude il piano più comune che mi sento proporre, e cioè che l'organizzazione IT di gruppo gestirà semplicemente il sito statunitense come

gestisce ogni altro sito. Un covered contractor information system è definito come "an unclassified information system that is owned, or operated by or for, a contractor", un sistema informativo non classificato posseduto da un contraente oppure gestito da esso o per suo conto, e che tratta, conserva o trasmette covered defense information. Gestito da esso o per suo conto. Se il reparto IT della Sua casa madre gestisce i Suoi sistemi statunitensi, quei sistemi sono covered contractor information system, e l'ambiente della casa madre non è fuori dalla Sua valutazione. È dentro. Affidare il lavoro al gruppo non sposta l'obbligo all'estero. Tira il gruppo dentro il perimetro.

La clausola porta con sé il resto della forma su cui deve pianificare:

- Implementare il NIST SP 800-171 sui covered contractor information system, nella revisione in vigore al momento in cui è emessa la richiesta di offerta, oppure come autorizzato dal Contracting Officer (DFARS 252.204-7012(b)(2)(i)). La revisione è agganciata alla richiesta di offerta, quindi delimiti l'insieme dei controlli sul contratto che ha davanti, e non sulla slide di un fornitore.
- Un fornitore esterno di servizi cloud che conserva, tratta o trasmette covered defense information deve soddisfare requisiti di sicurezza equivalenti alla baseline FedRAMP Moderate, e rispettare i paragrafi della clausola su segnalazione degli incidenti informatici, software malevolo, conservazione dei supporti, accesso forense e valutazione dei danni (DFARS 252.204-7012(b)(2)(ii)(D)). Se l'hosting del gruppo è quel fornitore, il gruppo sta sottoscrivendo tutto quanto.
- Segnalare un incidente informatico entro 72 ore dalla scoperta. La clausola definisce "rapidly report" esattamente così. Un servizio di assistenza gestito dalla casa madre a cinque fusi orari di distanza rientra ora nel Suo conto alla rovescia di 72 ore, il che è una questione di organico prima ancora che di conformità.
- La clausola si trasmette a cascata ai subcontratti senza modifiche, salvo che per identificare le parti (DFARS 252.204-7012(m)). Le consociate del gruppo non ne sono esenti per il fatto di condividere il Suo logo.
- La CMMC Level 2 significa i 110 requisiti di sicurezza del NIST SP 800-171, e da luglio 2026 vi si arriva con un'autovalutazione ogni tre anni e un'attestazione annuale nel sistema SPRS (il sistema statunitense di valutazione del rischio dei fornitori). Il 13 luglio 2026 il Dipartimento ha sospeso l'obbligo di certificazione da parte di un organismo terzo previsto dalla Fase II e ha aperto una revisione per riformare il programma. La clausola qui sopra non si è mossa, quindi una nuova operazione statunitense non può comunque trattare il confine come un progetto da secondo anno. Ciò che è cambiato è chi dichiara che i controlli sono in funzione. Ora è Lei.

> **Gestito da esso o per suo conto. Se il reparto IT della casa madre gestisce i Suoi sistemi, i sistemi della casa madre sono dentro la Sua valutazione CMMC. Centralizzare presso il gruppo non sposta l'obbligo all'estero. Tira il gruppo dentro il confine.**

Il confine non si ferma agli uffici

Tutto quanto finora è facile da immaginare come un problema d'ufficio. Cartelle condivise, caselle di posta, un ERP, un servizio di assistenza. È esattamente in questa cornice che le officine a controllo estero falliscono, perché i dati controllati compiono i loro viaggi più pericolosi in reparto.

Nel momento in cui un disegno esce dall'ERP e diventa un'istruzione di lavoro alla macchina, il dato tecnico è passato da un sistema che Lei tratta come protetto a un sistema che storicamente ha trattato come una macchina e non come un computer. Il file CAM sul PC condiviso di reparto. Il programma che risiede sul controllore. Il data historian che registra i dati di processo legati a un pezzo controllato, e poi si sincronizza con un server che tutto l'ufficio può raggiungere. Per un'officina domestica, quel passaggio è già il punto di controllo più trascurato dell'edificio. Per un'officina a controllo estero, ognuno di quei passaggi porta con sé una seconda domanda impilata sulla prima: non solo se questo dato sia controllato, ma chi nel gruppo possa raggiungere il sistema su cui è finito.

L'esempio che rende tutto questo concreto non è un cattivo. È il Suo miglior tecnico dell'automazione. Una linea si ferma a Nashua alle 2 del mattino. Il tecnico dei controlli della casa madre a Torino ha messo in servizio esattamente quella cella quattro volte e può rimetterla in moto in venti minuti con una sessione remota. È una foreign person. Il controllore contiene un programma derivato da dati tecnici controllati. Quella sessione remota è l'intera norma dentro una condivisione dello schermo, e il capoturno prenderà quella decisione alle 2 del mattino, a meno che l'architettura non l'abbia già presa per lui.

Quindi il confine si progetta dentro il reparto anziché tracciarlo attorno. Segmenti la rete OT affinché un endpoint d'ufficio raggiungibile non sia un percorso verso un controllore. Instradi i passaggi di consegne necessari attraverso un canale controllato e tracciato invece che su una chiavetta USB. Decida in anticipo, per iscritto, quali celle contengono programmi controllati e chi può raggiungerle, così che la decisione delle 2 del mattino sia una consultazione e non un giudizio da formulare sul momento. E dove l'assistenza tecnica del gruppo è davvero la risposta giusta, la faccia autorizzare come si deve tramite il consulente legale mentre la linea sta ancora girando, invece di scoprire la domanda durante un incidente.

È per questo che tratto il confine dei dati e il modello operativo come un unico problema di progettazione anziché due. Lo stesso filo convergente che dà a un valutatore un unico percorso verificabile dal contratto al truciolo è il filo che dà al P&L una visione onesta di ciò che il reparto sta davvero facendo. Costruito una volta sola, è la prova per l'auditor e il cruscotto del titolare. Costruito due volte, sono due sistemi che si contraddicono.

> **Alla norma non importa che fossero le 2 del mattino e che la linea fosse ferma. Decida chi può raggiungere un controllore che contiene un programma controllato prima della notte in cui la linea si ferma, e smette di essere una decisione che spetta al capoturno.**

L'organigramma conserva due bandiere

Ogni casa madre sente il confine dei dati riservato ai US-person come un muro tra sé e la società che possiede. Quella lettura uccide più progetti di questo tipo di quanti ne uccida qualunque controllo, ed è sbagliata. Costruito come si deve, la casa madre non perde quasi nulla di ciò che le serve davvero.

Torni alla definizione. I dati tecnici ai sensi dell'ITAR sono le informazioni necessarie a progettare, fabbricare, collaudare, riparare o modificare un defense article, e il 22 CFR 120.33(b) esclude espressamente le informazioni di marketing di base su funzione o finalità e le descrizioni generali di sistema. Il bilancio consolidato non è un dato tecnico. L'acquisizione ordini, il portafoglio ordini, la puntualità delle consegne, il tasso di scarto, la produttività oraria, l'organico, gli investimenti, gli indicatori di qualità e la lavagna SQDIP non sono dati tecnici. Quasi nulla di ciò che il consiglio di una casa madre esamina davvero un martedì è un dato tecnico.

Quindi il compito di progettazione è preciso, ed è un compito operativo prima che giuridico: dare alla casa madre ogni numero a cui ha diritto, e nessuno dei disegni a cui non ha diritto. In pratica lo strato della reportistica è costruito per attraversare il confine e lo strato dell'ingegneria è costruito per non attraversarlo. È quella distinzione a costituire l'intera architettura, ed è il motivo per cui questo si decide in fase di progettazione, quando costa una conversazione, e non in fase di valutazione, quando costa un cambio di piattaforma.

- Attraversa il confine per progettazione: il bilancio consolidato, l'acquisizione ordini e il portafoglio ordini, la puntualità delle consegne, lo scarto e la resa, la produttività oraria, l'organico, gli investimenti, e la cadenza SQDIP (sicurezza, qualità, consegne, scorte, produttività). Il consiglio della casa madre conserva la sua riunione del martedì.
- Resta dentro il confine: i disegni, le specifiche, i programmi CAM e di collaudo, i fogli di processo, e ogni file derivato necessario a fabbricare, collaudare o riparare l'articolo (22 CFR 120.33(a)).
- Restano dentro il confine: le chiavi. Le chiavi di decifratura, i codici di accesso alla rete e le password sono access information (22 CFR 120.55), e fornirle a una foreign person richiede un'autorizzazione (22 CFR 120.56(b)).
- Nominati, e messi per iscritto: un amministratore di sistema con status di US person per l'enclave, un responsabile nominativo con status di US person della decisione sugli accessi, e una matrice degli accessi ai dati tecnici che indichi, per ruolo e per cittadinanza, chi può raggiungere i dati controllati e chi no. L'auditor di un contraente principale e un revisore della DDTC (la direzione statunitense per il controllo del commercio della difesa) chiedono entrambi quella matrice. Un'intesa verbale non è un documento.
- Domanda distinta, calendario distinto: FOCI. La mitigazione FOCI è ciò che la DCSA (l'agenzia statunitense per il controspionaggio e la sicurezza della difesa) richiede quando una società a controllo estero ha bisogno dell'idoneità ad accedere a informazioni classificate, ed è negoziata tramite il Suo consulente legale specializzato in impianti abilitati. La maggior parte della produzione di difesa in subfornitura è lavoro non classificato su CUI (informazioni controllate non classificate) e su dati soggetti a controllo ITAR, che non richiede affatto una facility clearance (il nulla osta di sicurezza dell'impianto). Quel lavoro ha comunque bisogno di questo confine dei dati fin dal primo giorno. Il FOCI è condizionato alla classe di lavori che

persegue. Il confine dei dati non è condizionato a nulla.

> **La casa madre conserva la società, la governance e ogni numero che il suo consiglio esamina. La filiale conserva i disegni. Non è un muro tra una casa madre e il suo investimento. È l'unica architettura sotto la quale quell'investimento si aggiudica il contratto.**

Ciò che costruisco io, e ciò che resta al consulente legale

Sono il partner delle operazioni, e sono preciso su dove si ferma quel confine. Metto in piedi e gestisco l'operazione statunitense conforme: il reparto produttivo, il modello operativo, la costruzione dell'ambiente IT e OT, il confine dei dati riservato ai US-person, e le prove di prontezza per il varco che sta rincorrendo. La costituzione dell'entità, la registrazione presso ITAR e DDTC, la mitigazione FOCI, le valutazioni su licenze ed esenzioni, e le questioni CFIUS (il comitato statunitense per gli investimenti esteri) restano di competenza del Suo consulente legale d'impresa e del Suo consulente in materia di controllo delle esportazioni. Mi coordino con loro e rispondo io del risultato operativo.

Quella linea non è modestia, è la ragione per cui il cantiere tiene. Se una specifica architettura rientri nella deroga del 22 CFR 120.54, se un determinato trasferimento richieda una licenza, se il Suo assetto proprietario faccia scattare una notifica alla DDTC: sono valutazioni giuridiche con conseguenze giuridiche. Un architetto delle operazioni che gliele risolve Le sta vendendo una responsabilità con una voce sicura. Quello che faccio io è costruire l'operazione affinché quelle valutazioni siano nette, documentate e semplici, e affinché le prove esistano prima che qualcuno le chieda.

Questo cantiere non è teorico e non è raro. Nell'aprile 2026 American Rheinmetall ha raggiunto la certificazione CMMC Level 2 in tutti i suoi siti produttivi statunitensi: un'operazione statunitense con casa madre tedesca che regge quella postura, agli atti pubblici. Sono stato io stesso l'operatore della casa madre estera negli Stati Uniti, dirigendo le operazioni nordamericane di una multinazionale italiana di sensori, e sto avviando ora le operazioni statunitensi di produzione per la difesa per la filiale di una casa madre canadese. La via esiste e c'è chi la sta percorrendo. Ciò che scarseggia è l'operatore che la percorre con Lei. Sei categorie di consulenti aiutano un produttore estero a entrare nel mercato statunitense, dai consulenti legali FOCI alla strutturazione delle Big Four alla selezione del sito ai fornitori IT per la CMMC, e ognuna di esse Le consegna un documento, un edificio o un certificato. La Standards Guide for Foreign Partners del Chief Information Officer del Dipartimento della Difesa è la cosa più vicina a una sintesi ufficiale, ed è uno strato di controlli anziché la sequenza di un operatore. Qualcuno deve comunque mettere in piedi e gestire l'operazione. Quello strato è il lavoro, ed è quello di cui rispondo io.

La sintesi è il titolo. La Sua casa madre è una foreign person rispetto ai dati tecnici della Sua filiale statunitense, quindi i disegni, i file derivati e le chiavi restano dentro un confine riservato ai US-person, mentre il testo cifrato, i dati finanziari e la governance lo attraversano liberamente. L'ITAR traccia quel confine, il NIST SP 800-171 lo tiene, e la CMMC Level 2 dimostra che tiene. Costruisca i tre come un solo filo e il valutatore trova i controlli già in funzione, perché sono il modo stesso in cui il lavoro viene svolto. Costruiscali come tre trattative con tre fornitori e scopre quale dei tre era sbagliato al varco, con il contratto sul tavolo. Un solo filo. Due bandiere.

La nostra casa madre è davvero una foreign person se ci possiede al 100 per cento?

Sì. Ai sensi dell'ITAR il criterio per un'entità è la costituzione societaria, non la proprietà. Una US person comprende qualunque entità costituita per operare negli Stati Uniti (22 CFR 120.62), e una foreign person comprende qualunque entità non costituita né organizzata per operare negli Stati Uniti (22 CFR 120.63). La Sua filiale statunitense è una US person. La Sua casa madre, costituita all'estero, è una foreign person. Possedere l'intera filiale non sposta né l'una né l'altra oltre quella linea, perché le definizioni non chiedono mai della proprietà. L'ITAR definisce separatamente la proprietà estera e il controllo estero al 22 CFR 120.65, e quelle definizioni contano per ciò che dichiara alla Directorate of Defense Trade Controls. Non creano un'eccezione familiare alle regole sui dati.

Il nostro sito statunitense può funzionare sull'ERP della casa madre?

Di norma non senza un confine. Se la Sua operazione statunitense detiene dati tecnici controllati, quei dati restano dentro un confine dei dati riservato ai US-person, quindi un'istanza condivisa che dia agli utenti lato casa madre un percorso verso disegni o specifiche è una questione di rilascio ai sensi del 22 CFR 120.56(a)(3), che ruota sul fatto che una foreign person possa essere messa in condizione di raggiungere dati tecnici non cifrati. A volte la risposta è un'istanza segregata, a volte un sistema separato, a volte un'interfaccia controllata che passa verso l'alto i dati di pianificazione e i dati finanziari mentre l'archivio di ingegneria resta dentro il confine. La decisione architetturale fa parte del cantiere, e si prende sui Suoi flussi di dati reali, non su un modello preconfezionato.

Cifrare tutto risolve il problema?

La cifratura risolve il problema del trasporto, non il problema dell'autorità. L'ITAR prevede una deroga reale al 22 CFR 120.54(a)(5) per l'invio, il trasporto o la conservazione di dati tecnici non classificati sotto cifratura end-to-end conforme al FIPS 140-2 o di robustezza comparabile, e il 22 CFR 120.54(c) conferma che la possibilità di accedere a dati correttamente cifrati non è né un rilascio né un'esportazione. Ma la deroga è definita in modo da richiedere che i mezzi di decifratura non siano forniti ad alcun terzo (22 CFR 120.54(b)(1)), e le chiavi di decifratura, i codici di accesso alla rete e le password sono access information ai sensi del 22 CFR 120.55. Le fornisca a una foreign person e si trova nel 22 CFR 120.56, un rilascio, e un'esportazione ai sensi del 22 CFR 120.50(a)(6). Quindi la casa madre può detenere il testo cifrato. La casa madre non può detenere la chiave. Se il Suo assetto specifico soddisfi ogni condizione della deroga è una valutazione che spetta al Suo consulente in materia di controllo delle esportazioni.

Il reparto IT della nostra casa madre può amministrare i nostri sistemi statunitensi?

Non senza tirare la casa madre dentro la Sua valutazione, e non senza rispondere prima alla domanda ITAR. Il DFARS 252.204-7012 definisce un covered contractor information system come un sistema posseduto da un contraente, oppure gestito da esso o per suo conto, che tratta, conserva o trasmette covered defense information. Se la casa madre gestisce i Suoi sistemi, quei sistemi sono covered contractor information system e l'ambiente della casa madre si trova dentro il perimetro della Sua CMMC. Separatamente, un amministratore che può reimpostare una password può mettere qualcuno in condizione di accedere a ciò che quella password protegge, ed è il criterio del rilascio del 22 CFR 120.56(a)(3). La risposta praticabile è di norma un'amministrazione dell'enclave affidata a US person, con il gruppo che resta interamente al di

fuori.

L'esenzione canadese permette alla nostra casa madre canadese di raggiungere i dati tecnici della nostra filiale statunitense?

No, ed è la lettura errata più comune nella corsia canadese. L'esenzione del 22 CFR 126.5 autorizza l'esportazione senza licenza di articoli e servizi non classificati della US Munitions List dagli Stati Uniti verso una persona registrata in Canada o verso un uso finale del governo canadese, con esclusioni, e con l'approvazione preventiva della Directorate of Defense Trade Controls richiesta per la riesportazione o il ritrasferimento. Autorizza un'esportazione, in una direzione, a determinate condizioni. Non concede a una casa madre canadese un diritto permanente di raggiungere i dati tecnici soggetti a ITAR detenuti dalla sua filiale statunitense. È esattamente per questa lettura errata che il confine dei dati riservato ai US-person viene costruito. Il Suo consulente in materia di controllo delle esportazioni conferma che cosa copra l'esenzione sui Suoi fatti concreti.

Serve la mitigazione FOCI prima di poter detenere dati tecnici soggetti a ITAR?

Sono due domande su due calendari diversi. La mitigazione FOCI è ciò che la Defense Counterintelligence and Security Agency richiede quando una società a controllo estero ha bisogno dell'idoneità ad accedere a informazioni classificate, ed è negoziata con la DCSA tramite il Suo consulente legale specializzato in impianti abilitati. La maggior parte della produzione di difesa in subfornitura è lavoro non classificato su CUI e su dati soggetti a controllo ITAR, che non richiede mai una facility clearance, quindi la mitigazione FOCI può non entrare mai nel Suo perimetro. Il confine dei dati riservato ai US-person funziona diversamente. Se detiene dati tecnici controllati, si applica dal primo giorno in cui li detiene. Sapere quale classe di lavori sta perseguendo è ciò che decide se il FOCI entri o meno nella conversazione.

La CMMC richiede cittadini statunitensi?

La CMMC non decide quella questione. I controlli di accesso del NIST SP 800-171 chiedono se un utente sia autorizzato, non quale passaporto abbia. L'ITAR è il regime che decide chi può essere autorizzato ad accedere a dati tecnici soggetti a controllo delle esportazioni, e una foreign person ha bisogno di una licenza o di un'esenzione. I due si compongono invece di competere: l'ITAR traccia la linea, i controlli 800-171 la impongono e la registrano, e la valutazione CMMC Level 2 misura se sia reale. È anche il motivo per cui costruirli come un unico programma funziona, e per cui costruirli come tre trattative con tre fornitori produce tre risposte che si contraddicono al varco.

Fonti

1. ITAR 22 CFR 120.63, foreign person (eCFR). Il criterio della costituzione societaria che rende una casa madre estera una foreign person rispetto alla sua stessa filiale statunitense
   https://www.ecfr.gov/current/title-22/section-120.63
2. ITAR 22 CFR 120.62, U.S. person (eCFR). Qualunque entità costituita per operare negli Stati Uniti
   https://www.ecfr.gov/current/title-22/section-120.62
3. ITAR 22 CFR 120.50, export, compreso il deemed export di dati tecnici a una foreign person negli Stati Uniti alla lettera (a)(2) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.50
4. ITAR 22 CFR 120.33, technical data. La definizione funzionale che si attiva senza alcuna marcatura (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.33
5. ITAR 22 CFR 120.54, attività che non sono esportazioni, compresa la deroga per la cifratura end-to-end alla lettera (a)(5) e la sua definizione alla lettera (b) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.54
6. ITAR 22 CFR 120.55, access information. Chiavi di decifratura, codici di accesso alla rete e password (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.55
7. ITAR 22 CFR 120.56, release. L'uso di access information per mettere una foreign person in condizione di raggiungere dati tecnici non cifrati (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.56
8. ITAR 22 CFR 120.65, proprietà estera e controllo estero, come l'ITAR li definisce per i propri fini (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.65
9. ITAR 22 CFR 126.5, esenzioni canadesi (eCFR), e i suoi limiti rispetto all'accesso della casa madre estera ai dati tecnici controllati
   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, clausola datata maggio 2024, aggiornata al 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, nella collocazione che il DFARS 252.204-7012(b)(2)(i) richiama
    https://csrc.nist.gov/publications/sp800
12. DoD CIO, About CMMC: la sospensione del 13 luglio 2026 dei requisiti della Fase II, la pausa nella Fase 1, e la CMMC Level 2 come autovalutazione ogni tre anni sui 110 requisiti del NIST SP 800-171 Revision 2 con attestazione annuale nel sistema SPRS, ai sensi della clausola DFARS 252.204-7012
    https://dodcio.defense.gov/CMMC/About/
13. DFARS 225.003 Definizioni, paesi qualificati (acquisition.gov, aggiornato al DFARS Change 5/7/2026)
    https://www.acquisition.gov/dfars/225.003-definitions.

14. DCSA, Foreign Ownership, Control, or Influence (FOCI) e mitigazione ai fini del nulla osta di sicurezza dell'impianto
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), lo strato di controlli per le operazioni statunitensi a controllo estero
https://dodcio.defense.gov/Portals/0/Documents/Library/StandardsGuideForeignPartners.pdf

16. American Rheinmetall raggiunge la certificazione CMMC Level 2 per i suoi siti produttivi statunitensi (14/04/2026)
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, il metodo operativo a quattro pilastri, e il pilastro Sovereign Tier dove si fissano i confini dei dati
/method

18. Il manuale d'ingresso nel mercato statunitense per i produttori alleati della difesa, la sequenza completa di avviamento operativo dentro cui questo documento si colloca
/resources/us-market-entry-playbook

19. La zona di atterraggio del New England, dove i fornitori alleati della difesa insediano le proprie operazioni statunitensi
/resources/new-england-landing-zone

20. Convergenza IT/OT per i produttori della difesa: perché MES, ERP e SCADA sono tre responsabilità di conformità finché non diventano una sola
/blog/it-ot-convergence-defense-manufacturers

21. Manuale di onshoring per il produttore estero: avviare operazioni statunitensi di produzione per la difesa in 90 giorni
/blog/foreign-manufacturer-onshoring-90-day-playbook

PROSSIMO PASSO

Richiedere un colloquio strategico

garrettpartridge.com/booking