CONFORMITÉ

Un seul fil, deux drapeaux : la frontière de données réservée aux US-persons dans une opération de défense à maison mère étrangère

Comment la frontière de données réservée aux US-persons, la frontière de données ITAR et la CMMC Level 2 se construisent en un seul fil numérique auditable à l'intérieur d'une opération américaine sous contrôle étranger.

Livre blanc · Garrett Partridge · 16 juillet 2026

garrettpartridge.com · Brookline, NH

LA RÉPONSE DIRECTE

Oui. Une filiale américaine sous contrôle étranger peut détenir des données techniques contrôlées au sens de l'ITAR et atteindre la CMMC Level 2. Aucun des deux régimes ne demande qui vous détient. Tous deux demandent où résident les données et qui peut les atteindre. Au titre de l'ITAR, votre filiale américaine est une US person parce qu'elle est constituée aux États-Unis, et votre maison mère est une foreign person parce qu'elle ne l'est pas (22 CFR 120.62 et 120.63). La détention du capital ne change ni l'une ni l'autre réponse. Communiquer des données techniques à une foreign person à l'intérieur des États-Unis est une exportation, une exportation réputée (deemed export, 22 CFR 120.50(a)(2)) : les ingénieurs, les administrateurs informatiques et le support de votre maison mère sont donc des destinataires étrangers des données de votre propre filiale, sauf si une licence ou une exemption en dispose autrement. La CMMC Level 2 exige ensuite les contrôles du NIST SP 800-171 sur les systèmes qui détiennent des CUI (informations non classifiées contrôlées), et la preuve que ces contrôles fonctionnent réellement. Ce que cela suppose en pratique, c'est un seul chantier, pas trois : une frontière unique réservée aux US-persons tracée autour des travaux contrôlés, la maison mère à l'extérieur, tenue par le contrôle d'accès, la segmentation et la journalisation que l'évaluateur note précisément. L'organigramme garde deux drapeaux. Le fil numérique n'en garde qu'un.

Votre maison mère est une foreign person

La phrase qui réorganise tout ce problème est courte, et la plupart des maisons mères l'entendent pour la première fois bien trop tard. Au titre de l'ITAR (le contrôle américain des exportations d'armement), votre maison mère est une foreign person (une personne étrangère au sens de l'ITAR) à l'égard des données techniques de votre filiale américaine. Pas un partenaire avec un peu de paperasse en plus. Une foreign person : la même catégorie que n'importe quelle autre entreprise à l'étranger ne détenant pas de licence.

La réglementation y parvient par la constitution en société, pas par la détention du capital. Une US person (une personne américaine au sens de l'ITAR) comprend toute entité « constituée pour exercer des activités aux États-Unis » (incorporated to do business in the United States, 22 CFR 120.62). Une foreign person comprend toute entité « non constituée ni organisée pour exercer des activités aux États-Unis » (not incorporated or organized to do business in the United States, 22 CFR 120.63). Votre entité du Delaware ou du Massachusetts est une US person. Votre maison mère à Ottawa, à Brescia ou à Stuttgart est une foreign person. Que la maison mère détienne 100 pour cent de la filiale ne fait franchir la ligne ni à l'une ni à l'autre. Il n'y a pas d'exception familiale dans le texte, parce que le texte ne pose jamais la question de la famille.

Les dirigeants entendent cela comme une insulte à une relation d'entreprise qu'ils ont mis des décennies à bâtir. Ce n'en est pas une. C'est un énoncé sur les données, et sur les données seulement. La maison mère détient toujours l'entreprise, nomme le conseil, fixe la stratégie et perçoit le profit. Ce que la maison mère cesse d'obtenir automatiquement, c'est le plan.

Le même réflexe se manifeste autour du statut d'allié, autant le refermer maintenant. Chaque pays

que je sers est un pays qualifié au sens du DFARS (supplément à la réglementation fédérale américaine sur les acquisitions de défense), dans le cadre d'un accord réciproque sur les marchés de défense conclu avec le Department of Defense (DFARS 225.003). Ce statut est une préférence dans les marchés publics, portant sur les produits finis et les composants. Il ne lève pas l'ITAR, il ne lève pas la CMMC, et il ne règle pas la question FOCI. Le statut d'allié fait passer vos pièces à travers l'analyse Buy American. Il ne fait pas passer votre maison mère à travers la frontière de données.

L'ITAR définit bien la détention étrangère et le contrôle étranger, pour ses propres besoins, au 22 CFR 120.65. La détention étrangère, c'est plus de 50 pour cent des titres de vote en circulation. Le contrôle étranger, c'est l'autorité ou la capacité d'établir ou d'orienter les politiques générales ou les opérations quotidiennes, et il est présumé lorsque des personnes étrangères détiennent 25 pour cent ou plus des titres de vote en circulation, sauf si une US person en contrôle un pourcentage égal ou supérieur. Ces définitions comptent pour ce que vous déclarez à la DDTC (direction américaine du contrôle du commerce de défense). Elles appartiennent à l'ITAR, et elles ne sont pas le cadre FOCI (propriété, contrôle ou influence étrangers) de la DCSA (l'agence américaine de contre-espionnage et de sécurité de la défense), lequel fonctionne selon des règles distinctes. Gardez les deux séparés, et laissez le conseil en contrôle des exportations et un spécialiste des relations avec la DCSA porter chacun leur moitié.

> **Le critère est la constitution en société, pas la détention du capital. Votre filiale américaine est une US person parce qu'elle est constituée ici. Votre maison mère est une foreign person parce qu'elle ne l'est pas. Détenir 100 pour cent de la filiale ne change ni l'une ni l'autre réponse.**

Ce qui se trouve réellement à l'intérieur de la frontière

Avant de pouvoir tracer une frontière, il faut savoir ce qu'elle contient. Deux populations de données sont en jeu. Elles se recouvrent largement, et la plupart des ateliers se trompent sur les deux exactement de la même manière : ils attendent un marquage.

Les données techniques au sens de l'ITAR sont les informations requises pour la conception, le développement, la production, la fabrication, l'assemblage, l'exploitation, la réparation, l'essai, la maintenance ou la modification d'un article de défense, y compris les informations sous forme de plans, de dessins, de photographies, de schémas, d'instructions ou de documentation (22 CFR 120.33(a)). Relisez cette définition et remarquez ce qui lui manque. Il n'y a aucun marquage dedans. Les données techniques se définissent par ce que l'information permet de faire, et non par le fait qu'un tampon ait atterri dans le coin de la page. Un fichier de FAO que personne n'a étiqueté est une donnée technique s'il est requis pour fabriquer la pièce.

Les informations de défense couvertes obéissent à une logique parallèle. Au titre du DFARS 252.204-7012, ce sont les informations techniques contrôlées non classifiées, ou d'autres informations du CUI Registry, qui exigent une protection et qui sont soit marquées ou identifiées dans le contrat, soit « collectées, développées, reçues, transmises, utilisées ou stockées par le contractant ou pour son compte dans le cadre de l'exécution du contrat ». Ce second volet n'exige pas davantage de marquage.

Ainsi, l'instruction selon laquelle vivent vos équipes, protéger ce qui est marqué, est la mauvaise instruction. Deux régimes, deux définitions, et aucun des deux n'attend d'autocollant. Tous deux s'attachent à la fonction et au contexte, ce qui est précisément la raison pour laquelle ils ne peuvent pas être délégués à qui manie le tampon.

- La donnée technique est fonctionnelle. Si l'information est requise pour concevoir, fabriquer, tester, réparer ou modifier l'article de défense, l'ITAR la traite comme une donnée technique, marquée ou non (22 CFR 120.33(a)).
- L'information de défense couverte est contextuelle. Une information utilisée ou stockée dans le cadre de l'exécution du contrat est une information de défense couverte, qu'elle soit arrivée marquée ou non (DFARS 252.204-7012, définitions).
- Les exclusions sont réelles, et elles sont utiles. Les données techniques au sens de l'ITAR ne comprennent pas les principes scientifiques, mathématiques ou d'ingénierie généraux couramment enseignés à l'université, les informations relevant du domaine public, ni les informations commerciales de base sur la fonction ou la finalité et les descriptions générales de systèmes d'articles de défense (22 CFR 120.33(b)). Cette exclusion est ce qui permet à votre maison mère de conserver son reporting, et j'y reviens à la fin.
- Ce sont les fichiers dérivés qui vous rattrapent. Le plan est évident et les gens le manipulent avec soin. Le fichier de FAO, le plan de montage, le programme de contrôle et la fiche de processus qui en dérivent sont ceux qui atterrissent discrètement sur un partage que personne n'a en charge.

> **Vos équipes ont été formées à chercher un marquage. La donnée technique au sens de l'ITAR n'en exige aucun, et le second volet de l'information de défense couverte n'en exige pas davantage. Cet écart est l'endroit où un atelier à maison mère étrangère fuit en premier.**

Les cinq architectures IT de groupe qui fuient

C'est la partie qui frappe le plus fort dans la salle. Le principal obstacle entre un fabricant allié et un contrat du DoD n'est généralement pas la réglementation. C'est l'architecture IT de groupe que la maison mère a passé quinze ans à normaliser, et dont elle est fière à juste titre.

Au titre du 22 CFR 120.56(a)(3), une donnée technique est communiquée par l'usage d'informations d'accès permettant de faire en sorte qu'une foreign person accède à des données techniques non chiffrées, les consulte ou les détienne, ou la mettant en mesure de le faire. Lisez le verbe. Mettre en mesure. La clause est écrite sur la capacité, pas sur l'intention, ni sur le fait que quelqu'un ait ouvert le fichier. Au titre du 22 CFR 120.56(b), une autorisation est requise pour fournir ces informations d'accès à une foreign person en premier lieu. La question que posent l'avocat en contrôle des exportations comme l'évaluateur n'est donc pas de savoir si la maison mère a regardé. C'est de savoir si la maison mère pouvait être mise en mesure de l'atteindre.

Cinq schémas rendent compte de l'essentiel de ce que je trouve lors d'une première visite :

- L'instance ERP ou PLM partagée. Un seul tenant de groupe, un seul référentiel articles, un seul coffre documentaire, et un bureau d'études côté maison mère disposant d'un accès en lecture sur l'ensemble. L'efficacité qui a justifié sa construction est précisément le problème.

- Le partage de fichiers de groupe. Un partage ou un tenant mondial où le site américain est un dossier. Les plans contrôlés y atterrissent parce que c'est là que les plans ont toujours atterri, et chaque utilisateur du groupe disposant d'un chemin vers ce dossier est une question d'accessibilité.
- Le support informatique délocalisé ou situé dans le pays de la maison mère. Le centre de services qui assiste chaque site, détient des droits d'administration sur chaque poste, et peut prendre la main à distance sur un poste de travail où un plan est ouvert. Le support est réellement bon. C'est pour cela qu'il a été centralisé.
- L'identité et le réseau hébergés par la maison mère. Le domaine de la maison mère, son VPN, ses administrateurs de domaine. Un administrateur qui peut réinitialiser n'importe quel mot de passe peut mettre en mesure d'accéder à tout ce que ce mot de passe protège. C'est le 22 CFR 120.56(a)(3) rédigé sous forme de fiche de poste.
- La sauvegarde et la reprise d'activité de groupe. Une réplication vers le centre de données de la maison mère, dont l'équipe stockage détient les clés de restauration. Personne ne pense à la sauvegarde comme à un chemin de données. C'est le chemin de données le plus complet du bâtiment.

> **La question n'est jamais de savoir si la maison mère a regardé le plan. Au titre du 22 CFR 120.56(a)(3), la question est de savoir si la maison mère pouvait être mise en mesure de l'atteindre. La capacité est le déclencheur, et la capacité d'un administrateur de domaine est totale par construction.**

Le chiffrement déplace les bits. Il ne déplace pas l'autorité.

La première idée que tout directeur technique compétent apporte à ce problème est le chiffrement, et l'intuition est juste. L'ITAR accorde au chiffrement une véritable exclusion. Cette exclusion est à la fois plus utile et plus étroite que presque tout le monde ne le croit, et l'écart entre ces deux lectures est l'endroit où les programmes deviennent coûteux.

Voici ce qu'elle accorde. Au titre du 22 CFR 120.54(a)(5), envoyer, emporter ou stocker des données techniques n'est pas une exportation lorsque les données sont non classifiées, sécurisées par un chiffrement de bout en bout, et sécurisées au moyen de modules cryptographiques conformes au FIPS 140-2 ou à ses successeurs, ou par d'autres moyens cryptographiques offrant une force de sécurité au moins comparable au minimum de 128 bits atteint par l'AES-128, et qu'elles ne sont ni intentionnellement envoyées à une personne se trouvant dans un pays proscrit au titre du 22 CFR 126.1, ni stockées dans un tel pays, ni envoyées depuis un tel pays. La règle règle même directement l'angoisse du routage : les données en transit par internet ne sont pas réputées stockées dans un pays qu'elles traversent. Et le 22 CFR 120.54(c) énonce clairement que la capacité d'accéder à des données techniques sous forme chiffrée répondant à ces critères ne constitue ni une communication ni une exportation.

Lisez maintenant la définition sur laquelle repose l'exclusion. À cette fin, le chiffrement de bout en bout exige que les données ne se trouvent pas sous forme non chiffrée entre l'expéditeur et le destinataire prévu, et que « les moyens de déchiffrement ne soient fournis à aucun tiers » (22 CFR 120.54(b)(1)). Le destinataire prévu doit être l'expéditeur, une US person se trouvant aux

États-Unis, ou une personne par ailleurs autorisée à recevoir les données techniques (22 CFR 120.54(b)(2)).

C'est là que cela s'effondre pour la plupart des architectures de groupe. Les informations d'accès sont définies au 22 CFR 120.55 comme les informations permettant d'accéder à des données techniques chiffrées sous forme non chiffrée, et la réglementation en nomme elle-même les exemples : les clés de déchiffrement, les codes d'accès réseau et les mots de passe. Fournissez-les à une foreign person et le 22 CFR 120.56(b) exige une autorisation pour le faire. Utilisez-les pour mettre une foreign person en mesure d'atteindre des données non chiffrées et vous êtes à l'intérieur du 22 CFR 120.56(a)(3), une communication. Et le 22 CFR 120.50(a)(6) fait de la communication de données techniques précédemment chiffrées une exportation à part entière.

L'architecture découle donc du texte, et c'est la thèse de ce document. Le chiffré peut traverser l'infrastructure du groupe. Les clés ne peuvent pas passer à la maison mère. Votre maison mère peut détenir le stockage, porter le trafic, posséder le tuyau et faire tourner la réplication, pour autant que ce qu'elle détient lui reste illisible et que les moyens de déchiffrement restent à l'intérieur de la frontière réservée aux US-persons. Cette seule asymétrie est ce qui permet à une entreprise de conserver une relation IT unique et deux drapeaux.

Deux mises en garde, et je les pense toutes les deux. Les conditions du 22 CFR 120.54(a)(5), auxquelles s'ajoute la définition du (b), sont cumulatives : elles doivent toutes tenir, sur vos faits réels, en même temps. Et le point de savoir si votre architecture précise remplit les conditions est une qualification juridique que fait votre conseil en contrôle des exportations, pas un architecte des opérations. Mon travail est de construire l'environnement de sorte que cette qualification soit nette, documentée et facile à trancher par l'affirmative. La qualification elle-même reste au conseil juridique, et je le dis lors de la première réunion plutôt que lors de la dernière.

> **Les bits peuvent passer. Les clés, non. Une maison mère qui ne détient que du chiffré, les moyens de déchiffrement ne lui étant jamais fournis, détient du stockage. Une maison mère qui détient la clé détient des données techniques.**

La CMMC ne trace pas la ligne. Elle prouve que la ligne est réelle.

La plupart des ateliers à maison mère étrangère mènent l'ITAR et la CMMC comme deux projets, avec deux prestataires et deux budgets, et souvent un troisième pour la construction du réseau. C'est un seul chantier. Comprendre pourquoi économise les six mois que ces programmes perdent d'ordinaire.

Le NIST SP 800-171 (le référentiel fédéral de protection des informations non classifiées contrôlées) est aveugle à la nationalité. Ses contrôles d'accès demandent si un utilisateur est autorisé. Ils ne demandent pas quel passeport il détient. Ce n'est pas une lacune de la norme, c'est une division du travail. L'ITAR est le régime qui décide qui peut être autorisé pour des données techniques sous contrôle d'exportation. Le NIST SP 800-171 est la machinerie qui applique la décision, la journalise et génère la preuve. La CMMC Level 2 est le Department of Defense qui vérifie que la machinerie est réelle.

Ce qui fixe la séquence. L'ITAR trace la frontière. Les contrôles 800-171 la tiennent. L'évaluateur la note. Construisez-les dans cet ordre et chacun alimente le suivant : la matrice d'accès que vous rédigez pour la question export devient le contrôle d'accès que l'évaluateur teste. Construisez-les comme trois conversations parallèles avec des prestataires et vous obtenez trois réponses qui se contredisent au moment du jalon.

Une définition à l'intérieur du DFARS 252.204-7012 met fin au plan le plus courant que j'entends, à savoir que le service informatique du groupe pilotera simplement le site américain comme il pilote tous les autres sites. Un covered contractor information system y est défini comme « un système d'information non classifié qui est détenu par un contractant, ou exploité par lui ou pour son compte » (owned, or operated by or for, a contractor) et qui traite, stocke ou transmet des informations de défense couvertes. Exploité par lui ou pour son compte. Si le service informatique de votre maison mère exploite vos systèmes américains, ces systèmes sont des covered contractor information systems, et l'environnement de la maison mère n'est pas hors de votre évaluation. Il est dedans. Confier le travail au groupe ne délocalise pas l'obligation. Cela fait entrer le groupe dans le périmètre.

La clause porte le reste de la forme qu'il faut anticiper :

- Mettre en oeuvre le NIST SP 800-171 sur les covered contractor information systems, dans la révision en vigueur au moment où l'appel d'offres est émis, ou telle qu'autorisée par le Contracting Officer (DFARS 252.204-7012(b)(2)(i)). La révision est arrimée à l'appel d'offres : calibrez donc le jeu de contrôles sur le contrat que vous avez devant vous, et non sur la diapositive d'un prestataire.
- Un prestataire de services cloud externe qui stocke, traite ou transmet des informations de défense couvertes doit satisfaire à des exigences de sécurité équivalentes au référentiel FedRAMP Moderate, et se conformer aux paragraphes de la clause portant sur la déclaration des incidents cyber, les logiciels malveillants, la préservation des supports, l'accès aux fins d'investigation et l'évaluation des dommages (DFARS 252.204-7012(b)(2)(ii)(D)). Si l'hébergement du groupe est ce prestataire, le groupe souscrit à tout cela.
- Déclarer un incident cyber dans les 72 heures suivant sa découverte. La clause définit « rapidly report » (déclarer rapidement) comme exactement cela. Un support informatique piloté par la maison mère à cinq fuseaux horaires de distance se trouve désormais à l'intérieur de votre délai de 72 heures, ce qui est une question d'effectifs avant d'être une question de conformité.
- La clause se répercute sur les contrats de sous-traitance sans modification, sauf pour identifier les parties (DFARS 252.204-7012(m)). Les filiales du groupe n'en sont pas exemptées parce qu'elles partagent votre logo.
- La CMMC Level 2 signifie les 110 exigences de sécurité du NIST SP 800-171, et, en juillet 2026, elle s'atteint par une auto-évaluation tous les trois ans assortie d'une attestation annuelle déposée dans le SPRS. Le 13 juillet 2026, le ministère a suspendu l'exigence de certification par un tiers de la Phase 2 et a ouvert une revue en vue d'une réforme. La clause ci-dessus n'a pas bougé : une nouvelle opération américaine ne peut donc toujours pas traiter la frontière comme un projet de deuxième année. Ce qui a changé, c'est qui énonce que les contrôles fonctionnent. C'est désormais vous.

> **Exploité par le contractant ou pour son compte. Si le service informatique de la maison mère pilote vos systèmes, les systèmes de la maison mère sont à l'intérieur de votre évaluation CMMC. Centraliser avec le groupe ne délocalise pas l'obligation. Cela fait entrer le groupe à l'intérieur de la frontière.**

La frontière ne s'arrête pas au bureau

Tout ce qui précède est facile à se représenter comme un problème de bureau. Des partages de fichiers, des boîtes aux lettres, un ERP, un support. Ce cadrage est précisément la manière dont les ateliers à maison mère étrangère échouent, car la donnée contrôlée effectue ses voyages les plus dangereux à l'atelier.

Dès l'instant où un plan quitte l'ERP et devient une instruction de travail à la machine, la donnée technique est passée d'un système que vous traitez comme protégé à un système que vous avez historiquement traité comme une machine plutôt que comme un ordinateur. Le fichier de FAO sur un PC d'atelier partagé. Le programme posé sur l'automate. L'historien qui journalise des données de procédé rattachées à une pièce contrôlée, puis se synchronise vers un serveur que tout le bureau peut atteindre. Pour un atelier domestique, ce passage est déjà le point de contrôle le plus négligé du bâtiment. Pour un atelier à maison mère étrangère, chacun de ces passages porte une seconde question empilée sur la première : non seulement s'agit-il d'une donnée contrôlée, mais qui, au niveau du groupe, peut atteindre le système sur lequel elle a atterri ?

L'exemple qui rend cela concret n'est pas un méchant. C'est votre meilleur ingénieur automaticien. Une ligne tombe à Nashua à 2 heures du matin. L'ingénieur de contrôle-commande de la maison mère, à Turin, a mis en service exactement cette cellule quatre fois et peut la remettre en marche en vingt minutes par une session à distance. Il est une foreign person. L'automate détient un programme dérivé de données techniques contrôlées. Cette session à distance, c'est toute la réglementation en un seul partage d'écran, et le responsable d'équipe va prendre cette décision à 2 heures du matin, à moins que l'architecture ne l'ait déjà prise pour lui.

La frontière se conçoit donc à l'intérieur de l'atelier plutôt qu'autour. Segmentez le réseau OT pour qu'un poste de bureau accessible ne soit pas un chemin vers un automate. Acheminez les transferts nécessaires par un conduit contrôlé et journalisé plutôt que par une clé USB. Décidez d'avance, par écrit, quelles cellules détiennent des programmes contrôlés et qui peut les atteindre, afin que la décision de 2 heures du matin soit une consultation et non un arbitrage. Et là où le support d'ingénierie du groupe est réellement la bonne réponse, faites-le autoriser dans les règles par le conseil juridique pendant que la ligne tourne encore, plutôt que de découvrir la question pendant un incident.

C'est pourquoi je traite la frontière de données et le modèle opérationnel comme un seul problème de conception et non deux. Le même fil convergé qui donne à un évaluateur un chemin auditable unique du contrat jusqu'à la coupe est le fil qui donne au compte de résultat une vue honnête de ce que fait réellement l'atelier. Construit une fois, il est la preuve de l'auditeur et le tableau de bord du dirigeant. Construit deux fois, ce sont deux systèmes qui se contredisent.

> La réglementation ne se soucie pas qu'il ait été 2 heures du matin et que la ligne ait été à l'arrêt. Décidez qui peut atteindre un automate détenant un programme contrôlé avant la nuit où la ligne tombe, et cela cesse d'être une décision que le responsable d'équipe doit prendre.

L'organigramme garde deux drapeaux

Chaque maison mère entend la frontière de données réservée aux US-persons comme un mur entre elle et l'entreprise qu'elle détient. Cette lecture tue plus de ces projets que n'importe quel contrôle, et elle est fausse. Bien construite, la maison mère ne perd presque rien de ce dont elle a réellement besoin.

Revenez à la définition. La donnée technique au sens de l'ITAR est l'information requise pour concevoir, fabriquer, tester, réparer ou modifier un article de défense, et le 22 CFR 120.33(b) exclut expressément les informations commerciales de base sur la fonction ou la finalité ainsi que les descriptions générales de systèmes. Les comptes consolidés ne sont pas des données techniques. Les prises de commandes, le carnet de commandes, la ponctualité de livraison, le taux de rebut, le débit, les effectifs, les investissements, les indicateurs qualité et le tableau SQDIP (sécurité, qualité, délais, en-cours, productivité) ne sont pas des données techniques. Presque rien de ce que le conseil d'une maison mère examine réellement un mardi n'est une donnée technique.

La tâche de conception est donc précise, et c'est une tâche opérationnelle plutôt que juridique : donner à la maison mère chaque chiffre auquel elle a droit, et aucun des plans auxquels elle n'a pas droit. En pratique, la couche de reporting est construite pour franchir la frontière et la couche d'ingénierie est construite pour ne pas la franchir. Cette distinction est toute l'architecture, et c'est pourquoi cela se décide au moment de la conception, où cela coûte une conversation, plutôt qu'au moment de l'évaluation, où cela coûte une refonte de plateforme.

- Franchit la frontière par conception : les comptes consolidés, les prises de commandes et le carnet de commandes, la ponctualité de livraison, le rebut et le rendement, le débit, les effectifs, les investissements, et la cadence SQDIP. Le conseil de la maison mère garde sa revue du mardi.
- Reste à l'intérieur de la frontière : les plans, les spécifications, les programmes de FAO et de contrôle, les fiches de processus, et chaque fichier dérivé requis pour fabriquer, tester ou réparer l'article (22 CFR 120.33(a)).
- Reste à l'intérieur de la frontière : les clés. Les clés de déchiffrement, les codes d'accès réseau et les mots de passe sont des informations d'accès (22 CFR 120.55), et les fournir à une foreign person exige une autorisation (22 CFR 120.56(b)).
- Nommé, et consigné par écrit : un administrateur système US-person pour l'enclave, un responsable US-person nommément désigné de la décision d'accès, et une matrice d'accès aux données techniques qui nomme, par rôle et par nationalité, qui peut atteindre les données contrôlées et qui ne le peut pas. L'auditeur d'un donneur d'ordres comme un examinateur de la DDTC demandent tous deux cette matrice. Une entente verbale n'est pas un artefact.
- Question distincte, calendrier distinct : le FOCI. L'atténuation FOCI est ce que la DCSA exige

lorsqu'une entreprise sous contrôle étranger a besoin d'être éligible à l'accès à des informations classifiées, négociée par votre conseil juridique spécialisé dans les établissements habilités. L'essentiel de la fabrication de défense en sous-traitance porte sur des travaux non classifiés, relevant des CUI et sous contrôle ITAR, qui n'exigent jamais de facility clearance (habilitation de sécurité d'établissement). Ces travaux exigent tout de même cette frontière de données dès le premier jour. Le FOCI est conditionné à la classe de travaux que vous visez. La frontière de données n'est conditionnée à rien du tout.

> **La maison mère garde l'entreprise, la gouvernance, et chaque chiffre que son conseil examine. La filiale garde les plans. Ce n'est pas un mur entre une maison mère et son investissement. C'est la seule architecture sous laquelle cet investissement remporte le contrat.**

Ce que je construis, et ce qui reste au conseil juridique

Je suis le partenaire des opérations, et je suis précis sur la limite de ce rôle. Je mets en place et je pilote l'opération américaine conforme : l'atelier, le modèle opérationnel, la construction de l'environnement IT et OT, la frontière de données réservée aux US-persons, et les preuves de préparation pour le jalon que vous cherchez à franchir. La constitution de l'entité, l'enregistrement ITAR et DDTC, l'atténuation FOCI, les qualifications de licence et d'exemption, et les questions CFIUS (le contrôle fédéral des investissements étrangers aux États-Unis) restent du ressort de votre conseil juridique d'entreprise et de votre conseil en contrôle des exportations. Je me coordonne avec eux et j'assume le résultat opérationnel.

Cette ligne n'est pas de la modestie, c'est la raison pour laquelle le chantier tient. Savoir si une architecture précise remplit les conditions de l'exclusion du 22 CFR 120.54, si un transfert précis exige une licence, si votre structure de détention déclenche une notification à la DDTC : ce sont des qualifications juridiques aux conséquences juridiques. Un architecte des opérations qui y répond à votre place vous vend un passif d'une voix assurée. Ce que je fais, c'est construire l'opération de sorte que ces qualifications soient nettes, documentées et faciles, et que la preuve existe avant que quiconque ne la demande.

Ce chantier n'est ni théorique ni rare. En avril 2026, American Rheinmetall a obtenu la certification CMMC Level 2 sur l'ensemble de ses sites de production américains : une opération américaine à maison mère allemande qui tient la posture, sur le registre public. J'ai moi-même été l'opérateur de la maison mère étrangère aux États-Unis, en dirigeant les opérations nord-américaines d'une multinationale italienne de capteurs, et je mets actuellement en place des opérations américaines de fabrication de défense pour la filiale d'une maison mère canadienne. La voie existe et des gens l'empruntent. Ce qui est rare, c'est l'opérateur qui l'emprunte avec vous. Six catégories de cabinets aideront un fabricant étranger à entrer sur le marché américain, du conseil juridique FOCI à la structuration Big Four en passant par le conseil en implantation et les prestataires IT spécialisés CMMC, et chacun d'eux vous remet un document, un bâtiment ou un certificat. Le Standards Guide for Foreign Partners du Chief Information Officer du DoD est ce qui se rapproche le plus d'une synthèse officielle, et c'est un référentiel de contrôles plutôt que la séquence d'un opérateur. Il reste à quelqu'un à mettre en place et à piloter l'opération. Cette couche est le travail, et c'est celle que j'assume.

La conclusion est dans le titre. Votre maison mère est une foreign person à l'égard des données techniques de votre filiale américaine : les plans, les fichiers dérivés et les clés restent donc à l'intérieur d'une frontière réservée aux US-persons, tandis que le chiffré, les comptes et la gouvernance la franchissent librement. L'ITAR trace cette frontière, le NIST SP 800-171 la tient, et la CMMC Level 2 prouve qu'elle tient. Construisez les trois en un seul fil et l'évaluateur trouve les contrôles déjà en fonctionnement, parce qu'ils sont la manière dont le travail se fait. Construisez-les comme trois conversations avec des prestataires et vous apprenez laquelle était fausse au moment du jalon, le contrat sur la table. Un seul fil. Deux drapeaux.

QUESTIONS FRÉQUENTES

Notre maison mère est-elle vraiment une foreign person si elle nous détient à 100 pour cent ?

Oui. Au titre de l'ITAR, le critère pour une entité est la constitution en société, pas la détention du capital. Une US person comprend toute entité constituée pour exercer des activités aux États-Unis (22 CFR 120.62), et une foreign person comprend toute entité non constituée ni organisée pour exercer des activités aux États-Unis (22 CFR 120.63). Votre filiale américaine est une US person. Votre maison mère, constituée à l'étranger, est une foreign person. Détenir la totalité de la filiale ne fait franchir la ligne ni à l'une ni à l'autre, car les définitions ne posent jamais la question de la détention. L'ITAR définit bien la détention étrangère et le contrôle étranger séparément, au 22 CFR 120.65, et ces définitions comptent pour ce que vous déclarez à la Directorate of Defense Trade Controls. Elles ne créent pas d'exception familiale aux règles sur les données.

Notre site américain peut-il fonctionner sur l'ERP de la maison mère ?

En général pas sans frontière. Si votre opération américaine détient des données techniques contrôlées, ces données restent à l'intérieur d'une frontière de données réservée aux US-persons : une instance partagée qui donnerait aux utilisateurs côté maison mère un chemin vers des plans ou des spécifications est donc une question de communication au titre du 22 CFR 120.56(a)(3), lequel se joue sur le point de savoir si une foreign person peut être mise en mesure d'atteindre des données techniques non chiffrées. Parfois la réponse est une instance ségréguée, parfois un système distinct, parfois une interface contrôlée qui fait remonter les données de planification et les données financières pendant que le coffre d'ingénierie reste à l'intérieur de la frontière. La décision d'architecture fait partie du chantier, et elle se prend au regard de vos flux de données réels plutôt que d'un modèle type.

Tout chiffrer règle-t-il le problème ?

Le chiffrement règle le problème du transport, pas celui de l'autorité. L'ITAR prévoit une véritable exclusion au 22 CFR 120.54(a)(5) pour l'envoi, l'export ou le stockage de données techniques non classifiées sous chiffrement de bout en bout répondant au FIPS 140-2 ou à une force comparable, et le 22 CFR 120.54(c) confirme que la capacité d'accéder à des données correctement chiffrées n'est ni une communication ni une exportation. Mais l'exclusion est définie de manière à exiger que les moyens de déchiffrement ne soient fournis à aucun tiers (22 CFR 120.54(b)(1)), et les clés de déchiffrement, les codes d'accès réseau et les mots de passe sont des informations d'accès au titre du 22 CFR 120.55. Fournissez-les à une foreign person et vous êtes dans le 22 CFR 120.56, une communication, et une exportation au titre du 22 CFR 120.50(a)(6). La maison mère peut donc détenir du chiffré. La maison mère ne peut pas détenir la

clé. Savoir si votre configuration précise satisfait à chacune des conditions de l'exclusion est une qualification pour votre conseil en contrôle des exportations.

Le service informatique de notre maison mère peut-il administrer nos systèmes américains ?

Pas sans faire entrer la maison mère dans votre évaluation, et pas sans répondre d'abord à la question ITAR. Le DFARS 252.204-7012 définit un covered contractor information system comme un système détenu par un contractant, ou exploité par lui ou pour son compte, qui traite, stocke ou transmet des informations de défense couvertes. Si la maison mère exploite vos systèmes, ces systèmes sont des covered contractor information systems et l'environnement de la maison mère se trouve à l'intérieur de votre périmètre CMMC. Séparément, un administrateur qui peut réinitialiser un mot de passe peut mettre en mesure d'accéder à ce que ce mot de passe protège, ce qui est le critère de communication du 22 CFR 120.56(a)(3). La réponse praticable est généralement une administration de l'enclave par des US persons, le groupe conservant tout ce qui se trouve à l'extérieur.

L'exemption canadienne permet-elle à notre maison mère canadienne d'atteindre les données techniques de notre filiale américaine ?

Non, et c'est la méprise la plus courante du couloir canadien. L'exemption du 22 CFR 126.5 autorise l'exportation sans licence d'articles et de services non classifiés de la US Munitions List depuis les États-Unis vers une Canadian-registered person ou vers une utilisation finale gouvernementale canadienne, avec des exclusions, et avec l'approbation préalable de la Directorate of Defense Trade Controls requise pour la réexportation ou le retransfert. Elle autorise une exportation, dans une direction, sous conditions. Elle n'accorde pas à une maison mère canadienne un droit permanent d'atteindre des données techniques ITAR détenues par sa filiale américaine. C'est précisément à cause de cette méprise que la frontière de données réservée aux US-persons se construit. Votre conseil en contrôle des exportations confirme ce que l'exemption couvre sur vos faits.

Avons-nous besoin d'une atténuation FOCI avant de pouvoir détenir des données techniques ITAR ?

Ce sont deux questions sur deux calendriers différents. L'atténuation FOCI est ce que la Defense Counterintelligence and Security Agency exige lorsqu'une entreprise sous contrôle étranger a besoin d'être éligible à l'accès à des informations classifiées, négociée avec la DCSA par votre conseil juridique spécialisé dans les établissements habilités. L'essentiel de la fabrication de défense en sous-traitance porte sur des travaux non classifiés, relevant des CUI et sous contrôle ITAR, qui n'exigent jamais de facility clearance : l'atténuation FOCI peut donc n'entrer jamais dans votre périmètre. La frontière de données réservée aux US-persons fonctionne autrement. Si vous détenez des données techniques contrôlées, elle s'applique dès le premier jour où vous les détenez. Savoir quelle classe de travaux vous visez est ce qui décide si le FOCI entre seulement dans la conversation.

La CMMC exige-t-elle des citoyens américains ?

La CMMC ne tranche pas cette question. Les contrôles d'accès du NIST SP 800-171 demandent si un utilisateur est autorisé, pas quel passeport il détient. L'ITAR est le régime qui décide qui peut être autorisé pour des données techniques sous contrôle d'exportation, et une foreign person a besoin d'une licence ou d'une exemption. Les deux se composent plutôt qu'ils ne se concurrencent : l'ITAR trace la ligne, les contrôles 800-171 l'appliquent et la journalisent, et

l'évaluation CMMC Level 2 note si elle est réelle. C'est aussi pourquoi les construire comme un seul programme fonctionne, et pourquoi les construire comme trois conversations avec des prestataires produit trois réponses qui se contredisent au moment du jalon.

Sources

1. ITAR 22 CFR 120.63, foreign person (eCFR). Le critère de constitution en société qui fait d'une maison mère étrangère une foreign person à l'égard de sa propre filiale américaine
   https://www.ecfr.gov/current/title-22/section-120.63
2. ITAR 22 CFR 120.62, U.S. person (eCFR). Toute entité constituée pour exercer des activités aux États-Unis
   https://www.ecfr.gov/current/title-22/section-120.62
3. ITAR 22 CFR 120.50, export, incluant l'exportation réputée de données techniques vers une foreign person aux États-Unis, au (a)(2) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.50
4. ITAR 22 CFR 120.33, technical data. La définition fonctionnelle qui s'attache sans marquage (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.33
5. ITAR 22 CFR 120.54, activities that are not exports, incluant l'exclusion pour chiffrement de bout en bout au (a)(5) et sa définition au (b) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.54
6. ITAR 22 CFR 120.55, access information. Les clés de déchiffrement, les codes d'accès réseau et les mots de passe (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.55
7. ITAR 22 CFR 120.56, release. L'usage d'informations d'accès pour mettre une foreign person en mesure d'atteindre des données techniques non chiffrées (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.56
8. ITAR 22 CFR 120.65, foreign ownership et foreign control, tels que l'ITAR les définit pour ses propres besoins (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.65
9. ITAR 22 CFR 126.5, les exemptions canadiennes (eCFR), et leurs limites quant à l'accès d'une maison mère étrangère aux données techniques contrôlées
   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 datée de mai 2024, à jour au 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, à l'emplacement que cite le DFARS 252.204-7012(b)(2)(i)
    https://csrc.nist.gov/publications/sp800
12. DoD CIO, About CMMC : la suspension du 13 juillet 2026 des exigences de la Phase 2, la pause en Phase 1, et la CMMC Level 2 comme auto-évaluation tous les trois ans face aux 110 exigences du NIST SP 800-171 Revision 2, avec attestation annuelle déposée dans le SPRS, au titre de la clause DFARS 252.204-7012
    https://dodcio.defense.gov/CMMC/About/

13. DFARS 225.003 Definitions, les pays qualifiés (acquisition.gov, à jour au DFARS Change 5/7/2026)
https://www.acquisition.gov/dfars/225.003-definitions.

14. DCSA, Foreign Ownership, Control, or Influence (FOCI) et l'atténuation en vue d'une facility clearance
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), le référentiel de contrôles applicable aux opérations américaines sous contrôle étranger
https://dodcio.defense.gov/Portals/0/Documents/Library/StandardsGuideForeignPartners.pdf

16. American Rheinmetall obtient la certification CMMC Level 2 pour ses sites de production américains (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, la méthode opérationnelle à quatre piliers, et le pilier Niveau souverain où se fixent les frontières de données
/method

18. Le manuel d'implantation sur le marché américain pour les fabricants de défense alliés, la séquence complète de mise en place dans laquelle ce document s'inscrit
/resources/us-market-entry-playbook

19. La zone d'atterrissage de la Nouvelle-Angleterre, là où les fournisseurs de défense alliés construisent leurs opérations américaines
/resources/new-england-landing-zone

20. Convergence IT/OT pour les fabricants de défense : pourquoi le MES, l'ERP et le SCADA sont trois passifs de conformité tant qu'ils n'en font pas un seul
/blog/it-ot-convergence-defense-manufacturers

21. Manuel d'implantation du fabricant étranger : mettre en place des opérations américaines de fabrication de défense en 90 jours
/blog/foreign-manufacturer-onshoring-90-day-playbook

PROCHAINE ÉTAPE

Demander un entretien stratégique

garrettpartridge.com/booking