



AIDE-MÉMOIRE

Outil pour les PME

Pour vous, propriétaire-dirigeant·e de PME manufacturière, technologique ou de services qui se demande si la défense est une avenue. Cet aide-mémoire vous aide à décider, à choisir votre porte d'entrée et à passer à l'action

La défense, est-ce pour vous ?

Ce n'est pas que des équipements militaires et des avions. Au sens de la Stratégie industrielle de défense du Canada (février 2026), la défense désigne l'ensemble de l'écosystème des industries et des organisations qui contribuent, directement ou indirectement, aux capacités de défense et de sécurité d'une nation. Trois grands segments de noyau (aérospatiale, fabrication spécialisée, spatial), huit secteurs de production industrielle (munitions, systèmes autonomes, soutien en service, protection du personnel, formation et simulation, capteurs, systèmes numériques) et des sous-secteurs transversaux (IA, quantique, minéraux critiques, biotechnologies, énergie, électronique, cybersécurité, manufacturier).

Les cinq catalyseurs depuis 2025

- Engagement 2 % → 5 % du PIB en dépenses de défense (engagements OTAN).
- Stratégie industrielle de défense du Canada (février 2026) : encadre les priorités d'achat et les retombées attendues.
- Agence d'investissement en défense (autonomie à l'automne 2026) : doit accélérer les achats au-delà de PSPC, surtout de 25 à 100 M\$.
- Politique « Buy Canadian » : contenu canadien exigé sur les projets de 25 M\$+ comportant plus de 250 000 \$ d'acier ou d'aluminium (jusqu'à 25 % de prime de prix tolérée).
- Ajustement des RIT : la part exigée de PME passerait d'environ 15 % à 30 %.



Le « non » avant le « oui » : ne mettez pas 70-80 % de votre chiffre d'affaires à risque pour une opportunité de défense. La défense doit s'ajouter à un cœur d'activité solide, pas le remplacer. La première vraie question n'est pas « comment entrer ? » mais « est-ce que ça a du sens pour MON entreprise ? ».

Les cinq portes d'entrée — laquelle est la vôtre ?

Il existe cinq voies distinctes. Chacune a ses exigences, son effort et ses délais. Choisissez-en une consciemment, souvent une seule à la fois.

Porte d'entrée	Pour qui
1. Vente directe	Produit civil mature « sur étagère » ou innovation prête à démontrer
2. Entrepreneur principal (« prime »)	Grandes PME structurées (CA > 20 M\$), reins financiers solides
3. Sous-traitance / fourniture de système	Équipementiers et systémiers (attention au « flow down »)
4. Chaîne d'approvisionnement	PME manufacturières et services techniques (la voie la plus accessible)
5. Innovation par les centres IDE	Startups et PME technologiques (IDEeS, DIANA, Minerva, Borealis)

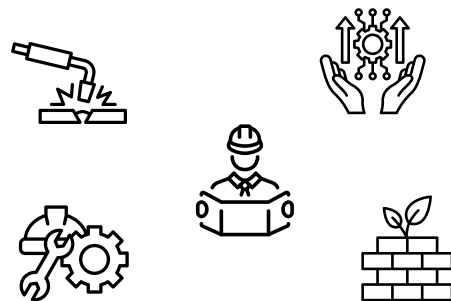


La porte la plus probable pour la majorité des PME : la porte 4 (chaîne d'approvisionnement). Plus vous êtes éloigné du donneur d'ordres (rang 2, 3, 4...), plus les exigences de certification diminuent. Étape obligatoire : vous inscrire aux registres fournisseurs des grands donneurs d'ordre ciblés.

La filière navale : un pilier stratégique de la défense

La filière navale regroupe un ensemble d'activités liées à la construction, la réparation, l'entretien, la modernisation, l'équipement, l'ingénierie, les technologies, la logistique et les services spécialisés associés aux navires et infrastructures maritimes. La filière navale peut être porteuse, mais elle comporte souvent des exigences élevées : cycles de vente plus longs, conformité, documentation, qualité, sécurité, traçabilité, cybersécurité et capacité à travailler avec des donneurs d'ordres ou des fournisseurs de rang supérieur. Pour une PME, les opportunités peuvent se situer à plusieurs niveaux :

- fabrication de pièces, composants ou sous-ensembles ;
- usinage, soudage, assemblage, finition ;
- équipements mécaniques, électriques ou électroniques ;
- automatisation, robotique, capteurs, logiciels, cybersécurité ;
- services d'ingénierie, conception, inspection, maintenance ;
- solutions environnementales, efficacité énergétique, matériaux ;
- formation, soutien technique, documentation, logistique.



Naval Québec publie un Guide de la chaîne d'approvisionnement navale du Québec, qui constitue une ressource de référence pour mieux comprendre les acteurs, les besoins et le fonctionnement de l'écosystème naval québécois.



N'hésitez pas à nous contacter pour toute précision supplémentaire, nous saurons vous aiguiller !



Ce document est une réalisation de
[l'Espace PME Innovation Chaudière-Appalaches](#)

Conditions de réussite

Pour réussir dans la filière, une PME doit généralement développer une combinaison de capacités.

1. Clarté de positionnement

L'entreprise doit être capable d'expliquer rapidement :

- ce qu'elle fait ;
- pour qui ;
- dans quelles conditions ;
- avec quelles preuves ;
- pourquoi son offre est pertinente pour la filière la défense. Choisir une seule porte d'entrée à la fois.

Question à poser :

Quelle problématique de défense, industrielle ou opérationnelle votre solution permet-elle de résoudre ?

2. Rigueur qualité

Démontrer la qualité, la constance et la traçabilité. ISO 9001 est souvent le socle ; AS9100 en aérospatiale. L'essentiel : un système qualité documenté et crédible.

3. Capacité documentaire

Les entreprises doivent souvent fournir :

- fiches techniques ;
- dessins ;
- procédures ;
- preuves de conformité ;
- certificats ;
- rapports d'inspection ;
- politiques qualité ;
- politiques de sécurité ;
- documents de traçabilité.

4. Compréhension des exigences de sécurité

Certains contrats peuvent toucher des informations, composantes ou données sensibles. Les entreprises qui examinent, possèdent ou transfèrent des marchandises contrôlées doivent s'inscrire au Programme des marchandises contrôlées du gouvernement du Canada. Les exigences peuvent inclure des évaluations de sécurité du personnel, des plans de sûreté, des inspections de conformité et le signalement d'atteintes à la sûreté.

5. Maturité numérique et cybersécurité

C'est la barrière à l'entrée n° 1. Le Programme canadien de certification en cybersécurité (PCCC), équivalent du CMMC américain, devient un prérequis — mais le niveau requis dépend de la position dans la chaîne et de l'information manipulée (CUI).

6. Patience commerciale

L'entreprise doit comprendre que l'entrée dans cette filière peut prendre du temps. Les premières retombées peuvent venir par :

- un contact avec un intégrateur ;
- une sous-traitance indirecte ;
- un petit mandat ;
- une participation à une rencontre B2B ;
- une inscription comme fournisseur ;
- une réponse à un appel d'intérêt ;
- une collaboration avec un donneur d'ordres ou un fournisseur existant.

Autodiagnostic : est-ce que j'ai un potentiel ?

Cochez. Si vous répondez « oui » à plusieurs questions de chaque bloc, vous avez un potentiel à explorer.

Mon offre et mon expertise	Oui	Non
Je fabrique, transforme, assemble, conçois ou intègre des produits techniques ?		
J'offre un service spécialisé utile à un chantier, un intégrateur ou un fournisseur ?		
Je travaille déjà avec des secteurs exigeants (transport, aéronautique, énergie, médical, industriel) ?		
Mon offre améliore la productivité, la qualité, la sécurité, la durabilité ou la résilience d'une chaîne ?		
Je peux adapter mon produit ou service à des exigences particulières ?		

Ma capacité opérationnelle	Oui	Non
Je peux documenter mes processus ?		
J'ai une capacité de production stable ?		
Je peux respecter délais, normes, plans, devis et exigences techniques ?		
Je peux gérer des demandes de soumission structurées ?		
J'ai une personne responsable de la qualité, de la conformité ou des opérations ?		
Je peux produire des preuves (fiches, certificats, rapports, traçabilité) ?		

Ma maturité commerciale et financière	Oui	Non
J'accepte d'entrer comme fournisseur de rang 2-3-4 avant de viser les grands donneurs d'ordre ?		
J'ai la capacité financière pour des cycles de vente longs ET pour la conformité initiale ?		
J'ai une proposition de valeur claire et des références clients solides ?		
Mon chiffre d'affaires est de l'ordre de quelques millions de dollars ?		
Je suis prêt à participer à des salons, rencontres B2B et démarches de qualification ?		

Phases d'un projet et délais réalistes

Le cycle complet d'un projet de défense, du besoin opérationnel à la livraison, s'étale typiquement sur 5 à 8 ans, avec au milieu la « vallée de la mort de l'innovation » (le besoin est identifié, mais le contrat tarde). Deux lectures : la chaîne existe déjà (un premier bon de commande en 12 à 24 mois en s'intégrant à un entrepreneur principal), mais une nouvelle technologie demande 5 à 8 ans.

Les trois phases

- 1** Phase de proposition (la plus stratégique) : le principal cherche encore qui pourra lui fournir quoi pour bâtir son contenu canadien. C'est là qu'il faut s'inscrire. Une fois l'appel d'offres ouvert, c'est trop tard.
- 2** Phase d'acquisition : le contrat est signé, les exigences deviennent rigides (ce qui est « build to print » ne se modifie plus).
Un cas réel : une entreprise a accepté un contrat sans réaliser que les dessins étaient en unités européennes, important de tout valider.
- 3** Phase de soutien en service (ISS) : jusqu'à 70 % de la valeur d'un projet, maintenance, retrofit, rétro-ingénierie, modernisation. Belle voie d'entrée pour l'usinage et l'électronique.

Décalage à la mi-2026 : il existe un écart entre les annonces budgétaires et la publication effective des appels d'offres. Les débloques rapides ont déjà eu lieu ; les nouveaux appels d'offres devraient s'accélérer à l'automne 2026 avec l'autonomie de l'Agence d'investissement en défense.

Les certifications : la règle d'or

Ne vous sur-certifiez pas. Le réflexe de courir vers la certification dès qu'on parle de défense est une erreur coûteuse. Plus vous êtes loin du donneur d'ordres, moins les exigences sont lourdes. Faites l'analyse d'écart AVANT d'investir, pour savoir quel niveau est réellement requis.

Cas concret (la règle d'or en action) : un fournisseur québécois en aérospatiale faisait affaire avec Safran, qui exigeait le PCCC/CMMC de tous ses fournisseurs. En creusant, on a constaté qu'aucune information sensible (CUI) n'était transmise dans cette relation : la certification n'était pas vraiment nécessaire. Toujours valider précisément ce qui est requis avant d'investir.

Certification	Ce que c'est
CMMC (É.-U.)	Cybersecurity Maturity Model Certification : programme du Département de la Guerre américain, trois niveaux, basé sur NIST 800-171 v2.
PCCC / CP-CSC (Canada)	Programme canadien de certification en cybersécurité : première mouture en avril 2026, basé sur NIST 800-171 v3. Réciprocité avec le CMMC annoncée mais pas en vigueur.
ITAR (É.-U.)	International Traffic in Arms Regulations : contrôle l'exportation/importation d'articles et services de défense.
PMC (Canada)	Programme des marchandises contrôlées : réglemente l'accès aux biens militaires et liés à la défense au Canada.
FedRAMP (É.-U.)	Standardise l'évaluation de sécurité des produits et services infonuagiques. Pertinent pour le numérique.
Directive SRI 2 / NIS 2 (UE)	Cybersécurité des secteurs critiques : à considérer pour l'expansion européenne.
ISO 9001 / AS9100	Normes générales de qualité (9001) et aérospatiales (AS9100).
ISO 14001	Norme environnementale, déjà demandée par certains donneurs d'ordre publics.

Le PCCC en détail (la certification clé au Canada)

Niveau	Exigences	Statut	Pour qui
Niveau 1	Autoévaluation (~17 points de contrôle)	En vigueur (avril 2026)	PME de rang 3-4-5, fournisseurs sans CUI
Niveau 2	98 points de contrôle, audit externe	À venir (2027)	Sous-traitants directs des primes manipulant de la CUI
Niveau 3	200 points de contrôle, audit externe	À venir (2028)	Primes et fournisseurs critiques sur projets stratégiques

La logique : protéger la CUI (Controlled Unclassified Information). Le but n'est pas de blinder toute l'entreprise, mais d'isoler la portion qui manipule de la CUI (postes dédiés, contrôles d'accès, ségrégation des systèmes). D'où l'intérêt, souvent, de séparer la division défense du reste de l'entreprise.

Feuille de route en 7 étapes

- 1** Diagnostic stratégique. Est-ce que la défense a du sens compte tenu de votre cœur d'activité, de votre alignement stratégique et de votre capacité d'investir ?
- 2** Choisir UNE porte d'entrée parmi les cinq. Vouloir entrer par plusieurs portes à la fois est une erreur classique.
- 3** S'inscrire aux registres fournisseurs des donneurs d'ordre ciblés. C'est gratuit et c'est souvent le premier filtre.
- 4** Faire l'analyse d'écart cybersécurité (NIST 800-171).
- 5** Mettre à niveau les certifications de base. Minimale ISO 9001 ; PCCC niveau 1 selon votre position ; niveau 2 ou 3 pour des contrats spécifiques.
- 6** Faire de la veille active. achatscanada.canada.ca, MERX, shipsforcanada.ca, portails des primes, événements CAF Outlook.
- 7** Participer à des salons sectoriels. DEFSEC Atlantic (priorité, accessible), CANSEC (le plus grand), événements régionaux.
Le but : rencontrer les acheteurs et identifier des partenaires.

N'hésitez pas à nous contacter pour toute précision supplémentaire, nous saurons vous aiguiller !



Ce document est une réalisation de
l'Espace PME Innovation Chaudière-Appalaches

Les trois pièges à éviter

- 1** La certification précipitée. Investir 200 000 \$ ou 400 000 \$ en cybersécurité sans avoir validé que c'est requis. L'analyse d'écart doit toujours précéder l'investissement.
- 2** Le « tout pour la défense ». Mettre à risque un cœur d'activité solide pour une opportunité incertaine. La défense s'ajoute, ne remplace pas.
- 3** L'attente passive. Espérer qu'un appel d'offres tombe dans votre boîte courriel. Le marché de la défense se conquiert « au corps à corps » : réseautage, portails, salons, accompagnement.

Par où commencer dès maintenant ?

- ✓ Rédiger une fiche de capacités claire (1 à 2 pages) : qui vous êtes, ce que vous offrez, vos preuves et vos différenciateurs.
- ✓ S'inscrire aux portails fournisseurs des donneurs d'ordre pertinents pour votre offre.
- ✓ Demander une rencontre ou un diagnostic à votre conseiller en développement économique ou autre expert reconnu.
- ✓ Cibler un salon à fréquenter cette année — DEFSEC Atlantic est le plus accessible pour débiter.
- ✓ Faire valider quelle porte d'entrée (1 à 5) vous convient avant d'investir.



ANNEXE — RÉFÉRENCES DÉTAILLÉES

Annexe 1 : Acteurs et donneurs d'ordre

Client final et mécanique d'achat

Le client ultime, ce sont les Forces armées canadiennes (Terre, Air, Marine, Spatial), qui expriment des besoins opérationnels. Trois entités gèrent l'achat : DND (besoins techniques et opérationnels), ISED (RIT et contenu canadien) et PSPC (publication des appels d'offres). La nouvelle Agence d'investissement en défense doit accélérer le processus dès l'automne 2026.

Grands donneurs d'ordre (« primes ») actifs au Canada

Donneur d'ordre	Domaine principal
Chantier Davie (Lévis)	Naval — brise-glaces polaires, frégates, navires de soutien
Irving Shipbuilding (Halifax)	Naval — destroyers River-class, navires de patrouille
General Dynamics Land Systems (London, ON)	Véhicules blindés terrestres
Rheinmetall (Canada/Europe)	Véhicules logistiques, remorqueurs (~100 véhicules)
Manac (Saint-Georges)	Remorques de défense (projet ~800 unités)
Soucy Defence (Drummondville)	Chenilles pour véhicules blindés (É.-U.)
Mack Defense (Saint-Nicolas)	Camions militaires (projet MSVS)
Groupe Océan (Québec)	Grands remorqueurs navals
Pomerleau (Saint-Georges)	Construction de centres de formation
Safran (Montréal)	Modernisation des périscopes des sous-marins Victoria
CAE (Montréal)	Formation et simulation
L3Harris (Mirabel)	Maintenance aéronautique

N'hésitez pas à nous contacter
pour toute précision supplémentaire,
nous saurons
vous aiguiller !



Ce document est une réalisation de
[l'Espace PME Innovation Chaudière-Appalaches](#)

Annexe 2 : Ressources

Plateformes officielles d'appels d'offres

- achatscanada.canada.ca; projets de défense (plateforme et équipement); 680+ projets par année prévus
- [MERX](#); appels d'offres d'infrastructure (rénovation des bases, etc.)
- shipsforcanada.ca (Irving); portail fournisseurs et Stratégie nationale de construction navale
- [Approvisionnement défense et marine](#); [SPAC](#); Programme des capacités de la Défense

Programmes d'innovation

- [Construction de Défense Canada](#) (CDC); DEC Développement économique Canada
- [Investissement Québec](#) / IQ International
- [IDeS](#); Innovation pour la défense, l'excellence et la sécurité
- [DIANA / OTAN](#) (hub Halifax); accélérateur d'innovation, taux de succès canadien élevé.
- [Recherche et développement pour la défense Canada](#) (RDDC)

Cadre stratégique et politiques

- [Stratégie industrielle de défense du Canada](#); Politique des retombées industrielles et technologiques (RIT)
- [État de l'industrie canadienne de la défense 2024](#); [Marchandises contrôlées : examen, possession ou transfert](#); page officielle PCCC (SPAC)

Associations, réseaux et cartographie

- [CADSI](#) (organise CANSEC)
- [FCCQ](#); Coalition québécoise pour la défense et la sécurité
- [Aéro Montréal](#); Chantier Défense et Sécurité
- [CDR Magazine](#) / Top 100 des entreprises canadiennes en défense (meilleure approximation d'un répertoire);
- [Canadian Defence Review](#); liste annuelle ISED des entreprises avec obligations RIT

Événements à mettre à l'agenda

- [CAF Outlook](#) (Canadian Armed Forces Outlooks); présentation par les Forces armées des projets à venir; idéal pour repérer les opportunités en amont
- [CANSEC](#) (Ottawa, fin mai); le plus grand salon de défense au Canada; coûteux, essentiel pour les acteurs établis
- [DEFSEC Atlantic](#) (Halifax, fin septembre); salon à taille humaine, très accessible, beaucoup de B2B; recommandé en priorité pour une PME qui débute

Accompagnement vers les certifications de cybersécurité PCCC et CMMC

[Cybereco](#)

N'hésitez pas à nous contacter
pour toute précision supplémentaire,
nous saurons
vous aiguiller !



Ce document est une réalisation de
[l'Espace PME Innovation Chaudière-Appalaches](#)