NORTHFLEET

GUIDE

Sept questions sur le logiciel

Pour qui achète ou accrédite des systèmes classifiés ou déconnectés

NOVEMBRE 2026 VERSION 1.0 · TLP:CLEAR northfleetsecurity.ca

RÉSUMÉ

Le logiciel d'un système classifié ou déconnecté continue d'arriver pendant des décennies après l'attribution du contrat. Voici sept questions à poser à qui le fournit, chacune avec ce qu'est une bonne réponse et la preuve à demander. Elles ont leur place dans les modalités d'un contrat, un énoncé des travaux ou une règle d'admission.

TABLE DES MATIÈRES

03 Pourquoi ces sept questions

03 Que contient-il, et qui livre chaque pièce?

04 À quoi chaque version est-elle comparée?

04 La vérification fonctionne-t-elle hors ligne?

05 Sauriez-vous que le lieu de compilation a changé?

05 Quel registre reste chez l'opérateur?

05 Que se passe-t-il le jour où les livraisons cessent?

06 Qu'est-ce qui échappe à ces vérifications?

07 Les sept questions sur une page

08 Où elles ont leur place

08 Sources

Pourquoi ces sept questions

Une bonne partie de ce que la Défense nationale achète contient du logiciel. En février 2026, la Stratégie industrielle de défense du Canada a prévenu que le contrôle exercé par l'étranger peut restreindre l'accès de l'utilisateur final « à la propriété intellectuelle, aux schémas et aux mises à jour logicielles nécessaires ». Elle a promis ceci : « Les décisions d'approvisionnement prises par l'AID [l'Agence de l'investissement pour la défense] comprendront des mesures visant à atténuer ces risques pour le contrôle souverain. »

Nous avons cherché ces mesures dans le budget fédéral et dans le projet de loi C-40, qui ferait de l'agence une société d'État, et nous ne les avons pas trouvées. Si l'agence demande à quoi ses « mesures visant à atténuer ces risques » devraient ressembler pour le logiciel, voici la liste que nous lui remettrions.

Ces questions s'adressent à quiconque achète, accrédite ou construit du logiciel destiné à un système classifié ou déconnecté. Chacune vient avec la réponse que nous espérons entendre et la preuve à demander.

Que contient-il, et qui livre chaque pièce?

Demandez la liste de tous les composants logiciels dont le système a besoin pour continuer de fonctionner, avec pour chacun qui le construit, qui le signe, d'où viennent ses mises à jour et le pays dont les lois pourraient en restreindre l'accès.

Le fournisseur devrait déjà l'avoir sous forme de document daté, et chaque composant de la nomenclature logicielle livrée avec la dernière version devrait y figurer. La plupart des lignes se trouveront hors du Canada. C'est le cas de la majorité des images de base, des bibliothèques et des outils de compilation, et personne ne va les déménager. Vous la lisez pour voir si le fournisseur sait quel pays pourrait restreindre chaque ligne, et quelles lignes un acheteur pourrait vérifier sans passer par leur propriétaire.

Le profil d'incidence moyenne du Centre canadien pour la cybersécurité, qui a remplacé son profil Protégé B en avril 2026, demande d'évaluer le préjudice qui découlerait d'une contrainte juridique externe (contrôle SA-400). Pour le logiciel, nous ferions partir cette évaluation de cette liste.

À quoi chaque version est-elle comparée?

L'opérateur devrait vérifier la signature du fournisseur avant toute installation, par rapport à une clé ou à une identité de signature qu'il a épinglée d'avance et obtenue par une autre voie que la version elle-même. La version devrait aussi être accompagnée d'une provenance, c'est-à-dire d'un document qui nomme le code source dont elle est issue et la compilation qui l'a produite.

Une empreinte lue sur le portail du fournisseur vient du même endroit que la version. Elle ne sert donc à rien si quelqu'un a altéré le portail. Si le fournisseur livre son propre outil de vérification, l'outil doit subir le même traitement, sans quoi il se porte garant de lui-même.

Demandez à voir le dossier de la dernière version reçue. Il devrait indiquer à quoi la version a été comparée, qui a fait la vérification et d'où venait la clé.

La vérification fonctionne-t-elle hors ligne?

Le profil d'incidence moyenne place le travail d'administration sur un poste sans accès à Internet (contrôle SI-400), et c'est sur ce poste qu'une version est appliquée. Le profil précise qu'il n'aborde pas les capacités des auteurs de menace dotés de moyens sophistiqués; il faut donc le voir comme un plancher. Pour les infrastructures essentielles, le Centre pour la cybersécurité demande aux exploitants d'« être prêts à isoler les systèmes pour une durée pouvant aller jusqu'à trois mois » et de prévoir une reconstruction au moyen « de copies et de sauvegardes immuables hors ligne de confiance ». Une vérification qui interroge un service de vérification, un serveur de licences ou un journal en ligne échoue dans les deux cas.

Le fournisseur devrait pouvoir énumérer ce qu'il faut avoir sur place pour que la vérification aboutisse : la version elle-même, sa provenance, les certificats racines et les clés qui servent à la vérifier, et une liste de révocation datée. Il devrait aussi savoir ce qui se passe quand un certificat de signature expire à la sixième semaine. Une bonne réponse : la signature est jugée à la date d'un horodatage signé qui accompagne la version.

Comme preuve, demandez une démonstration. Débranchez le câble, reconstruisez un système avec ce qui est sur place et notez tout ce qui cherche à joindre le réseau.

Sauriez-vous que le lieu de compilation a changé?

La signature du fournisseur se vérifie tout aussi bien après que le fournisseur a été compromis ou contraint. Une provenance signée par un service de compilation que le fournisseur n'exploite pas couvre un cas précis : une version qui porte la signature du fournisseur, mais qui a été compilée ailleurs. Sa provenance nomme un autre service de compilation, et une vérification épinglée sur ce service et sur le dépôt de code source échoue. Elle ne couvre pas une modification qui passe par le code source et la compilation habituels; la dernière question y revient. Demandez quel service de compilation signe la provenance, et aux lois de quel pays ce service est soumis.

Demandez ensuite si le contrat oblige le fournisseur à vous prévenir quand l'entreprise est vendue, quand une clé de signature ou la plateforme de compilation change, ou quand une dépendance change de mains. Si la réponse est oui, demandez quelle clause. Quoi que le contrat prévoie déjà en cas de changement de propriétaire, vérifiez que cela s'étend à la clé, à la plateforme de compilation et aux dépendances. Le pouvoir que prévoit le projet de loi C-40 d'exclure un soumissionnaire d'un processus concurrentiel viserait ce qui est proposé au dépôt de la soumission, et le logiciel continue d'arriver pendant des décennies après l'attribution.

Quel registre reste chez l'opérateur?

Chaque version reçue devrait laisser, dans les systèmes de l'opérateur, une entrée datée indiquant ce qui est arrivé, à quoi cela a été comparé, qui l'a approuvé et où cela a été installé. L'opérateur devrait pouvoir produire la liste de toutes les versions jamais reçues sans appeler le fournisseur ni ouvrir une session sur son portail.

Un accréditeur voudra ce registre de toute façon. Quand une mauvaise version est découverte plus tard, c'est aussi ce registre qui montre où elle a été installée. Demandez les entrées du dernier trimestre.

Que se passe-t-il le jour où les livraisons cessent?

Des fournisseurs sont vendus et des produits sont abandonnés. Le logiciel a-t-il besoin d'une licence renouvelée pour continuer de fonctionner, et que fait-il le lendemain de l'expiration de la licence? La dernière bonne version se trouve-t-elle chez l'opérateur? Pendant combien de

temps le système a-t-il été conçu et mis à l'essai pour fonctionner sans nouveaux correctifs, et selon quelles hypothèses?

L'entiercement est une réponse courante pour le long terme, et ses modalités méritent d'être lues. Vérifiez si le code source est remis quand le soutien cesse, et si le dépôt est tenu à jour. Vérifiez aussi si le dépôt contient tout ce qu'il faut pour une reconstruction, chaîne de compilation et bibliothèques comprises, et si quelqu'un du côté de l'acheteur saurait mener cette reconstruction.

Qu'est-ce qui échappe à ces vérifications?

Une version qui était mauvaise quand le fournisseur l'a compilée réussit toutes les vérifications ci-dessus. Il en va de même d'une porte dérobée écrite dans le code source, ou d'une version provenant d'un nouveau propriétaire qui a gardé la clé et le service de compilation et qui a changé le code.

Recompiler à partir du code source et comparer permet de repérer une version qui ne correspond pas à son code source, mais seulement pour un logiciel dont la compilation donne deux fois le même résultat, et à condition de faire confiance aux outils qui servent à recompiler. Une porte dérobée dans le code source se compile sans erreur dans les deux cas. Pour la trouver, il faut que quelqu'un lise le code. Dans le cas d'un logiciel à code source fermé, l'acheteur ne peut faire ni l'un ni l'autre, sauf si le contrat le prévoit.

De bonnes réponses aux six premières questions donnent à l'opérateur son mot à dire sur le moment où une version est installée, et un registre de l'endroit où elle l'a été. Faites davantage confiance à un fournisseur qui vous dit ce qui échappe à ses vérifications avant que vous le demandiez.

Les sept questions sur une page

N°	QUESTION	UNE BONNE RÉPONSE	DEMANDEZ À VOIR
1	**Que contient-il, et qui livre chaque pièce?**	Une liste datée de tous les composants : qui construit chacun, qui le signe, d'où viennent ses mises à jour et le pays dont les lois pourraient en restreindre l'accès.	La liste, à côté de la nomenclature logicielle de la dernière version.
2	**À quoi chaque version est-elle comparée?**	La signature du fournisseur, vérifiée par rapport à une clé ou à une identité de signature que l'opérateur a épinglée d'avance et obtenue par une autre voie. Une provenance qui nomme le code source et la compilation.	Le dossier de la dernière version reçue.
3	**La vérification fonctionne-t-elle hors ligne?**	La liste de ce qu'il faut avoir sur place, et une signature jugée à la date d'un horodatage signé, pour qu'un certificat puisse expirer pendant que le système est isolé.	Un système reconstruit avec ce qui est sur place, câble débranché, et la liste de tout ce qui a cherché à joindre le réseau.
4	**Sauriez-vous que le lieu de compilation a changé?**	Une provenance signée par un service de compilation que le fournisseur n'exploite pas, vérifiée par rapport à un service et à un dépôt de code source épinglés, et un contrat qui exige un avis en cas de vente ou de changement de clé, de plateforme de compilation ou de propriétaire d'une dépendance.	Le nom du service de compilation, les lois auxquelles il est soumis, et la clause.
5	**Quel registre reste chez l'opérateur?**	Une entrée datée pour chaque version, dans les systèmes de l'opérateur.	Les entrées du dernier trimestre, produites sans le fournisseur.
6	**Que se passe-t-il le jour où les livraisons cessent?**	Un comportement connu à l'expiration de la licence, la dernière bonne version chez l'opérateur, une durée de fonctionnement sans correctifs mise à l'essai, et un entiercement qui remet le code source quand le soutien cesse et qui contient tout ce qu'il faut pour une reconstruction.	Les modalités de l'entiercement, et la dernière bonne version chez l'opérateur.
7	**Qu'est-ce qui échappe à ces vérifications?**	Un fournisseur qui nomme ce que ses vérifications ne repèrent pas.	Pour un logiciel à code source fermé, les modalités du contrat qui permettent à l'acheteur de recompiler à partir du code source ou de lire le code.

Où elles ont leur place

Nous ne pensons pas qu'une seule des sept exige de modifier le projet de loi C-40. Elles ont leur place dans les modalités d'un contrat, un énoncé des travaux ou une règle d'admission, et un fournisseur peut préparer ses réponses avant qu'on les lui demande.

À propos de Northfleet. Northfleet est un fournisseur constitué en société au Canada qui bâtit la chaîne d'approvisionnement souveraine entourant un cluster classifié exploité par le client : un protocole d'ensembles pour le déploiement, une chaîne d'attestation et une piste d'audit qui révèle toute altération. L'architecture prévoit que les équipes de génie habilitées du client exploitent le cluster avec leurs propres clés. Northfleet ne détient aucune donnée client ni aucune clé de signature client. Chaque version que Northfleet livre porte une provenance qui la lie au code source à partir duquel elle a été construite, et le client peut la vérifier sans la participation de Northfleet. L'architecture suppose que le fournisseur peut être compromis ou contraint. Contraindre Northfleet ne produit donc pas de porte dérobée silencieuse, mais pour en déceler une, il faut que quelqu'un vérifie réellement les versions par rapport à leur code source et lise ce code.

Faites parvenir vos corrections à corrections@northfleetsecurity.ca. Pour discuter de ces questions, ou de vos propres réponses, écrivez-nous à northfleetsecurity.ca/fr/contact.

Sources

Défense nationale, Sécurité, souveraineté et prospérité : la Stratégie industrielle de défense du Canada, 17 février 2026. Pilier II, sous « ACHETER : Acquérir auprès d'autres avec un réinvestissement national et un contrôle souverain ».

Centre canadien pour la cybersécurité, Proposition de profil d'activités et de contrôles organisationnels de sécurité et de protection de la vie privée – Incidence moyenne (ITSP.10.033-01), avril 2026. Contrôles SA-400 et SI-400.

Projet de loi C-40, première lecture, 6 octobre 2026. Modifications à la Loi sur la production de défense, art. 29.

Centre canadien pour la cybersécurité, Initiative Résilience des infrastructures essentielles face à l'intensification des menaces, page modifiée le 18 septembre 2026.

Notes de terrain de Northfleet, en anglais, à northfleetsecurity.ca/field-notes. Chacune cite ses propres sources.

- Who holds the switch, 26 août 2026. Le registre de l'opérateur.
- Already in the rulebook, 18 septembre 2026. Le texte des contrôles du profil.
- How far down the supply chain, 28 octobre 2026. La liste des composants.
- What Europe will ask Canada to prove, 3 novembre 2026. La liste des composants.

- Federal budget: masters of our destiny, software updates sold separately, 5 novembre 2026. Le budget et le projet de loi C-40.
- Three months offline, 10 novembre 2026. Ce qui cherche à joindre le réseau.
- Palantir at DND: who checks the updates?, 11 novembre 2026. Clés, empreintes et portails.
- Buy Canadian: owned here, built where?, 16 novembre 2026. Compilation, ventes et entiercement.
- Defence industry at committee: seven questions about the software, 19 novembre 2026. La note dont ce guide est tiré.

© 2026 Sécurité Northfleet Ltée. Ce guide peut être reproduit et diffusé dans son intégralité. Il décrit les orientations publiques à la date indiquée et ne constitue pas un conseil portant sur un système en particulier.