Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.\11, rue Laurier
Gatineau
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires
Une exigence de sécurité est associée à ce document.

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Business Transformation and Systems Integration
Service/Division de transformation des opérations et d'intégrat
Special Procurement Initiative Dir
Dir. des initiatives speciales d'approvisionnement
11 Laurier, Place du Portage III
12C1
Gatineau
Québec
KIA 0S5

Title - Sujet Transformation de la SSI - DP	
Solicitation No. - N° de l'invitation EP243-170549/B	**Amendment No. - N° modif.** 009
Client Reference No. - N° de référence du client 20170549	**Date** 2017-08-16
GETS Reference No. - N° de référence de SEAG PW-$$XE-678-31237	
File No. - N° de dossier 678xe.EP243-170549	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2017-08-25**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Oates, Christine	**Buyer Id - Id de l'acheteur** 678xe
Telephone No. - N° de téléphone (873) 469-3917 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature**	**Date**

Canada

Modification n° 009

Objectif :

A. Recenser les modifications apportées à la DP.
B. Répondre aux questions reçues en ce qui concerne la présente DP.

A. MODIFICATIONS

Changement n° 87 :

À l'ANNEXE A, Partie 3 – Exigences techniques, sous 1.2 Exigences techniques :

SUPPRIMER :

Tech. 34	Sous la supervision du GC, élaborer des plans d'architecture physique et logique détaillés en utilisant les modèles du GC, et réaliser la solution à partir de l'architecture conceptuelle ainsi établie.

INSÉRER :

Tech. 34	Élaborer des plans d'architecture logique et physique de l'ISST (à l'aide de modèles GC) en fonction du modèle d'architecture conceptuelle ISST. Ces plans sont soumis à l'approbation du GC.

Changement n° 88:

Pièce jointe 1 de la partie 4 – Évaluation technique, article 4 – Critères cotés C1, sous l'entête Critères Cotés, **SUPPRIMER** le deuxième paragraphe au complet et le **REMPLACER** avec ce qui suit :

> Le Canada évaluera le plan préliminaire de gestion du projet par le soumissionnaire, selon le degré auquel il satisfait les éléments demandés suivants et la façon dont il favorise l'atteinte des résultats escomptés et respecte les contraintes énumérées dans les sections 1 à 7, ANNEX A:

Changement n° 89:

Pièce jointe 1 de la partie 4 – Évaluation technique, article 4 – Critères cotés C4, sous l'entête Pointage maximal:

SUPPRIMER :

Pointage maximum : 360

Pointage maximum de la partie A : 120

Pointage maximum de la partie B : 80

Pointage maximum de la partie C : 80

Pointage maximum de la partie D : 80

INSÉRER :

Pointage maximum : 360

Pointage maximum de la partie A : 90

SC.47 a) Trois parties, 10 pts chaques
SC.47 b) Quinze parties, 4 pts chaques

Pointage maximum de la partie B : 120

SC.16 Trois parties, 40 pts chaques

Pointage maximum de la partie C : 75

SC.9 a) Un partie, 75 pts

Pointage maximum de la partie D : 75

SC.42 a) Un partie, 26 pts
SC.42 b) Un partie, 25 pts
SC.42 c) Quatre parties, 6 pts chaques

Changement n° 90:

Pièce jointe 1 de la partie 4 – Évaluation technique, article 4 – Critères cotés C9, sous l'entête Critères cotés, **SUPPRIMER** le second paragraphe au complet et le **REMPLACER** avec ce qui suit :

> Aux fins de la présente évaluation, la gestion de cas se définit comme la gestion des activités, entre autres la mise au point, la coordination, la recherche, le soutien et l'exécution d'une demande de service d'un client, jusqu'à sa résolution. Le Portail Web de produits logiciels commerciaux est défini comme un ensemble de logiciels disponible sur le marché (en vente libre) qui fournit une composante d'échange vertical de données avec le public sur Internet (sur place) de la solution qui s'intègre à la plateforme de gestion des cas (sur place) et sert d'interface libre-service centrale et habilitante permettant les communications et les interactions.

B. QUESTIONS

Question nº 143 :

Dans la pièce jointe 1 de la partie 4 – Critères d'évaluation technique, 3. Critère coté C4 – Gestion de la sécurité, l'exigence indique :

« Le document devrait mettre l'accent sur les exigences en matière de sécurité, comme elles sont indiquées dans la section réservée aux exigences en matière de sécurité de la partie 4 de l'annexe A. Le Canada évaluera dans quelle mesure l'approche du soumissionnaire à l'égard de la gestion de la sécurité tient compte des contrôles de sécurité requis. Plus particulièrement, l'approche devrait :

A. Comprendre une description générale de bout en bout des opérations de sécurité; »

Le soumissionnaire n'est pas responsable de la gestion de la sécurité opérationnelle de la solution, et la DP ne comporte aucune précision sur les environnements de TI du Canada, comme la manière dont ils sont sécurisés, surveillés et la manière dont le Canada traite les incidents de sécurité à l'interne.

Le Canada envisagera-t-il de modifier cette exigence pour la rendre conforme au rôle du soumissionnaire (p. ex., le soumissionnaire ne joue aucun rôle sur le plan des opérations de sécurité de la solution, ni sur le plan de l'environnement de TI qui les prend en charge)?

Réponse nº 143 :

Il incombe a l'entrepreneur d'aider le gouvernement du Canada à mettre en œuvre les exigences relatives à la sécurité figurant dans l'énoncé des travaux. Aux fins de l'évaluation de l'expérience du soumissionnaire dans la mise en œuvre de la sécurité, le gouvernement du Canada demande que le soumissionnaire fournisse des scénarios opérationnels faisant état de l'application de contrôles de sécurité, tel qu'il est énoncé dans la section 4 Exigences en matière de sécurité de l'ANNEXE A. Il convient de noter que des précisons ont été apportées aux critères d'évaluation technique du critère C4 dans à la réponse à la question 73 de la modification 004. L'élément d'évaluation A auquel on faisait référence dans la question a été supprimé.

Question nº 144 :

Dans la pièce jointe 1 de la partie 4 – Critères d'évaluation technique, 3. Critère coté C4 – Gestion de la sécurité, l'exigence indique :

« Se reporter à toutes les parties de la section SC-01, Contrôle d'accès et gestion des comptes, et les aborder ».

Le soumissionnaire n'assurera ni la création ni la gestion des comptes et de l'accès.

Le Canada envisagera-t-il de modifier cette exigence pour permettre au soumissionnaire de décrire les capacités techniques de la solution et la configuration permettant l'interaction avec les utilisateurs et les opérateurs, conformément aux normes du GC?

Réponse nº 144 :

En ce qui a trait à la création et à la gestion de comptes ou d'accès, le gouvernement du Canada confirme que l'entrepreneur doit respecter les exigences de SC.01, tel qu'il est indiqué dans l'énoncé des travaux.

En ce qui a trait à la responsabilité, l'entrepreneur doit configurer la solution pour créer et gérer les comptes et l'accès. Cela comprend la création du premier compte et la validation des autorisations et de l'accès. Le gouvernement du Canada assurera la création et la maintenance de tous les comptes subséquents.

Des précisions ont été apportées au critère C4, et des modifications ont été apportées aux contrôles de sécurité auxquels on faisait référence. Les soumissionnaires doivent consulter le critère C4 révisé présenté à la question 50 de la Modification 004.

Question nº 145 :

Dans la pièce jointe 1 de la partie 4 – Critères d'évaluation technique, 3. Critère coté C4 – Gestion de la sécurité, l'exigence indique :

« Se reporter à toutes les parties de la section SC-07, Identification et authentification dans le document sur les opérations de sécurité, et les aborder**. »**

Le soumissionnaire ne sera pas responsable des justificatifs et des systèmes d'authentification.

Le Canada envisagera-t-il de modifier cette exigence pour permettre au soumissionnaire de décrire la manière dont la solution tirera avantage des justificatifs et des identités fournis et gérés par le GC, à titre d'autorité opérationnelle, conformément aux normes du GC?

Réponse nº 145 :

En ce qui a trait à l'identification et à l'authentification, le gouvernement du Canada confirme que la solution doit répondre aux exigences de SC.07, tel qu'il est indiqué dans l'énoncé des travaux. L'entrepreneur doit s'assurer que la solution peut identifier et authentifier avec succès et de façon unique les utilisateurs et que les mécanismes d'authentification satisfont aux normes indiquées. Des précisions ont été apportées au critère C4, et des modifications ont été apportées aux contrôles de sécurité auxquels on faisait référence. Les soumissionnaires doivent consulter le critère C4 révisé présenté à la question 50 de la Modification 004.

Question nº 146 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.32 (page 51 de 77). L'entrepreneur doit, pour la durée du contrat, apporter son aide au GC et intervenir en cas d'incident présumé ou réel lié à la solution.

Il s'agit d'un risque financier non lié puisqu'il est impossible d'estimer le nombre d'incidents pour lesquels cette exigence serait requise et l'inclure dans l'estimation d'une soumission. Ces données dépendent entièrement de la position de sécurité de l'ensemble de l'environnement de TI, de la granularité des détections de sécurité de SPC et de l'environnement de menace changeant.
Le Canada envisagera-t-il de modifier cette exigence afin que cette aide fasse l'objet d'une facturation distincte à titre de service professionnel offert après la mise en service, ou d'indiquer un nombre maximal de cas (et de jours d'effort pour chaque cas) afin qu'il soit possible d'établir une estimation et une tarification en conséquence?

Réponse nº 146 :

En ce qui a trait à la section SC.32, les travaux attendus consistent à offrir des services dans un environnement après l'entrée en service, car l'environnement de développement ne sera pas relié à Internet. Pendant cette période, l'entrepreneur sera responsable des incidents causés par une erreur ou une omission dans les travaux qu'il aura exécutés. De plus, l'entrepreneur doit respecter l'article 05 des conditions générales 2035, selon lesquelles « Tous les services rendus en vertu du contrat devront, au moment de l'acceptation, être libres de vices d'exécution et satisfaire aux exigences du présent contrat. Si l'entrepreneur doit corriger ou remplacer les travaux ou une partie de ceux-ci, il le fera à ses frais.»

Si des travaux qui ne tombent pas dans le champ de compétence susmentionné sont exigés de l'entrepreneur par le GC, ce dernier demandera des services facultatifs par le biais d'une autorisation de tâche.

Question nº 147 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.34 (page 51 de 77). L'entrepreneur doit, pour la durée du contrat, apporter son appui et son aide au GC avec la mise en œuvre des mesures d'atténuation (p. ex. blocage à l'aide du pare-feu, signatures personnalisées des services de détection et de prévention d'intrusion, suppression des logiciels malveillants) afin de maîtriser un incident de sécurité, d'assurer une protection contre les cybermenaces et d'éliminer les vulnérabilités, à la demande des représentants autorisés de TPSGC, selon les directives du Ministère et conformément au niveau de priorité du Canada.

Il s'agit d'un risque financier non lié puisqu'il est impossible d'estimer le nombre d'incidents pour lesquels cette exigence serait requise et l'inclure dans l'estimation d'une soumission. Ces données dépendent entièrement de la position de sécurité de l'ensemble de l'environnement de TI, de la granularité des détections de sécurité de SPC et de l'environnement de menace changeant.
Le Canada envisagera-t-il de modifier cette exigence afin que cette aide fasse l'objet d'une facturation

distincte à titre de service professionnel offert après la mise en service, ou d'indiquer un nombre maximal de cas (et de jours d'effort pour chaque cas) afin qu'il soit possible d'établir une estimation et une tarification en conséquence?

Réponse nº 147 :

L'entrepreneur est responsable des risques anticipés liés à la sécurité qui nécessitent des mesures d'atténuation évaluées pendant la conception et le développement de la solution. L'entrepreneur doit livrer l'architecture logique et physique conformément à la section Tech.34, architecture qu'il doit inclure dans les mesures d'atténuation de la conception du système pour ces occurrences anticipées. Pour l'atténuation des incidents après l'entrée en service, se reporter à la question 146 de la présente modification 009.

Question nº 148 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.36 (page 51 de 77). L'entrepreneur doit, pour la durée du contrat, apporter son appui et son aide à la préparation d'un rapport rétrospectif sur l'incident de sécurité, à la demande de TPSGC.

Il s'agit d'un risque financier non lié puisqu'il est impossible d'estimer le nombre d'incidents pour lesquels cette exigence serait requise et l'inclure dans l'estimation d'une soumission. Ces données dépendent entièrement de la position de sécurité de l'ensemble de l'environnement de TI, de la granularité des détections de sécurité de SPC et de l'environnement de menace changeant.
Le Canada envisagera-t-il de modifier cette exigence afin que cette aide fasse l'objet d'une facturation distincte à titre de service professionnel offert après la mise en service, ou d'indiquer un nombre maximal de cas (et de jours d'effort pour chaque cas) afin qu'il soit possible d'établir une estimation et une tarification en conséquence?

Réponse nº 148 :

Veuillez consulter la réponse à la question 146 dans la présente modification 009.

Question nº 149 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.40 (page 52 de 77). L'entrepreneur doit, pour la durée du contrat, installer des correctifs ou mettre en œuvre des mesures correctives dans le cadre de l'évaluation de la vulnérabilité. L'entrepreneur doit créer un dossier de demande de service pour les correctifs ou les mesures correctives qui ne peuvent être mis en œuvre dans le cadre de l'évaluation de la vulnérabilité.

À moins que le Canada ait l'intention d'accorder au soumissionnaire un contrat de service d'entretien du système pour la durée du contrat, cet aspect relève habituellement de l'autorité opérationnelle de TI, avec un soutien de deuxième et troisième ligne propre à la solution offert par le soumissionnaire, au besoin.

Le Canada pourrait-il clarifier cette exigence?

Réponse nº 149 :

À la lumière des résultats de l'évaluation de la vulnérabilité effectuée par le gouvernement du Canada, l'entrepreneur doit appliquer des correctifs et des mesures correctives dans la portée de la solution pour la durée du contrat. Dans l'éventualité où l'entrepreneur n'est pas en mesure de le faire en raison de facteurs comme une restriction de l'accès, il devra utiliser le processus de gestion des changements de TPSGC pour assurer la mise en œuvre des correctifs et des mesures correctives par le gouvernement du Canada par l'intermédiaire de dossiers de demande de service. Tous les changements doivent être rigoureusement documentés.

Question nº 150 :

La question 36 concerne la portée des contrôles de sécurité demandés par l'État et les éléments à inclure dans la solution et ceux à exclure de celle-ci. Dans sa réponse, l'État fait référence à la réponse de la question 35. Voici la réponse à cette question : « Veuillez prendre note que les contrôles de l'ITSG-33 ne seront pas tous mis en œuvre par l'entrepreneur. Il est à noter que plusieurs des technologies à intégrer sont mises en œuvre et ont des contrôles de sécurité en place. De même, les contrôles/exigences de sécurité pertinents pour l'infrastructure seront mis en œuvre par Services partagés Canada. L'EDT contient seulement les exigences qui nécessitent des efforts de la part de l'entrepreneur. »

D'après la réponse ci-dessus, l'exigence SC.38 indique que l'entrepreneur doit, pour la durée du contrat, apporter son appui et son aide au GC pour le maintien du niveau de sécurité de la solution en s'employant constamment à relever les problèmes suivants et à en informer le GC :

(a) les menaces et les vulnérabilités;

(b) les activités malveillantes et les accès non autorisés. La mise en œuvre incombe à l'entrepreneur dans le cadre de la solution.

Il va sans dire que l'exigence SC.38 incombe à SPC, qui doit surveiller les menaces et les vulnérabilités ainsi que les activités malveillantes et les accès non autorisés, en fonction des moyens mis en œuvre dans la solution, comme celui énoncé à l'exigence SC.04 : « produire des dossiers de vérification pour les incidents de sécurité dans un format pouvant être soumis dans le système de gestion des événements et des informations de sécurité ». On peut présumer qu'un tel système serait géré par SPC.

L'État fournira-t-il une matrice claire des responsabilités liées aux contrôles de sécurité dans la demande de proposition? Cette mesure vise à ce que l'entrepreneur et SPC puissent :

- éliminer le chevauchement des capacités de la solution et des coûts connexes pour l'État;
- indiquer clairement la portée de la solution et des services de sécurité de l'entrepreneur;
- tirer largement profit des responsabilités et des capacités actuelles de SPC.

Réponse nº 150 :

La modification 003 comporte une mise à jour du profil de sensibilité de la solution et des ajouts subséquents aux contrôles de sécurité, qui sont expliqués plus en détail dans la modification 008. Comme on l'a observé, de nombreux contrôles de sécurité doivent être pris en considération, soit les contrôles qui appuient les composants sensibles du profil PB/M/M et les contrôles supplémentaires qui répondent aux préoccupations récemment ajoutées quant aux éléments sensibles du profil PB/H/M. Les contrôles dont la mise en œuvre dans la solution relève de l'entrepreneur sont représentés comme exigences techniques dans l'énoncé des travaux. L'entrepreneur est tenu de satisfaire à l'ensemble des exigences techniques; autrement dit, il doit mettre en œuvre les contrôles représentés par les exigences techniques.

De plus, l'entrepreneur présentera une architecture physique globale dans laquelle sera indiquée l'inclusion générale de tous les contrôles. L'entrepreneur ne doit pas fournir les contrôles qui vont au-delà de la portée de ses travaux, mais doit tenir compte de l'incidence de ces contrôles dans la configuration et la construction de la solution visée par la portée de ses travaux.

Le gouvernement du Canada peut demander à l'entrepreneur de l'aider dans la mise en œuvre de contrôles hors de la portée des travaux lorsque celle-ci exige la participation de multiples équipes. Ce travail pourrait être réalisé aux termes d'une demande de changement.

Question nº 151 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.50 (page 53 de 77). L'entrepreneur doit, pour la durée du contrat, apporter son soutien et son aide au GC pour effectuer une vérification de l'installation des composants de sécurité conformément au plan de vérification de l'installation des composants de sécurité approuvé.

Il est difficile d'estimer les coûts en fonction de cette formulation.

Cette exigence s'applique-t-elle uniquement aux mises à jour de logiciels fournies par le soumissionnaire? Dans la négative, le Canada peut-il indiquer les types d'activités qu'il aimerait que le soumissionnaire inclue de façon permanente et le nombre de cas par année (ou le nombre de jours d'effort)?

Réponse nº 151 :

Pour la durée du contrat, l'entrepreneur doit fournir soutien et aide au gouvernement du Canada, conformément à SC.50, dans la réalisation de la vérification de l'installation de sécurité uniquement pour les éléments de solution fournis, préparés ou configurés par l'entrepreneur. La vérification de l'installation de sécurité doit être réalisée après chaque installation au cours de la mise en œuvre. Il peut être nécessaire de répéter la vérification de l'installation de sécurité lorsque des mises à niveau de la plateforme nuisent aux contrôles de sécurité de la solution fournie par l'entrepreneur.

Question nº 152 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.51. L'entrepreneur doit corriger les erreurs et omissions ayant trait à l'installation ou à la configuration relevées dans le cadre de la vérification de l'installation des composants de sécurité.

Conformément à la section SC.50. Il est difficile d'estimer les coûts en fonction de cette formulation.

Cette exigence s'applique-t-elle uniquement aux mises à jour de logiciels fournies par le soumissionnaire? Dans la négative, le Canada peut-il indiquer les types d'activités qu'il aimerait que le soumissionnaire inclue de façon permanente et le nombre de cas par année (ou le nombre de jours d'effort)?

Réponse nº 152 :

La vérification de l'installation de sécurité doit être réalisée par le gouvernement du Canada avec l'aide de l'entrepreneur avant la date de mise en service. Le gouvernement du Canada définit le soutien comme toute correction d'une erreur ou d'une omission dans l'installation ou la configuration se rapportant au travail de l'entrepreneur. Veuillez vous référer à la réponse à la question 146 de la présente modification 009 pour les erreurs ou omissions dans l'installation et la configuration survenant après la mise en service.

Question nº 153 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.41 (page 52 de 77). La solution doit, à tout le moins, satisfaire aux exigences du profil PB/M/M défini à l'annexe 4A du document ITSG-33, (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg33-ann4a-1-eng_4.pdf).

Le profil PB/M/M par défaut prévu au document ITSG-33 ne vise pas uniquement la prestation de solutions d'application par un entrepreneur. Il comprend environ 430 contrôles qui s'ajoutent à ceux prévus dans la DP, dont bon nombre vont au-delà de la portée apparente du rôle du soumissionnaire. Cette exigence élargira de façon exponentielle la portée de l'évaluation et de l'autorisation de sécurité.

L'incertitude à cet égard causera de la confusion au cours de l'évaluation et de l'autorisation de sécurité et entraînera pour les soumissionnaires un risque qui devra, au bout du compte, être couvert par des coûts dans l'estimation aux fins de la soumission.

Le Canada pourrait-il indiquer les contrôles prévus dans ce profil qui sont la responsabilité contractuelle du soumissionnaire, ceux qui relèvent du Canada et ceux qui ne s'appliquent pas (le cas échéant)?

Réponse nº 153 :

Veuillez consulter la réponse à la question 150 dans la présente modification.

Question nº 154 :

Dans l'appendice 2 de l'annexe A (Activités principales), le calendrier indique que les jalons « Planification et analyse » et « Conception de la solution » doivent être terminés d'ici la fin de décembre 2017. Notre approche propose la révision et l'approbation des recommandations du jalon « Planification et analyse » par le chargé de projet de TSSI avant d'effectuer les activités relatives à la « Conception de la solution ». De plus, celle-ci devra être approuvée par TSSI avant que les produits livrables soient considérés comme terminés.

L'achèvement de ces deux jalons d'ici la fin de décembre 2017 n'est peut-être pas possible.

Si notre plan global vise août 2018 comme échéance du jalon « Mise au point de la solution et configuration », pouvons-nous faire en sorte que les dates clés des jalons « Planification et analyse » et « Conception de la solution » soient flexibles?

Réponse nº 154 :

Le calendrier des jalons, dans l'APPENDICE 2 de l'ANNEXE A, a été présenté pour décrire le calendrier du projet et lorsque des étapes sont attendues. En préparation de leur offre, le soumissionnaire peut proposer de nouveaux échéanciers pour le calendrier des jalons tant et aussi longtemps que les activités essentielles indiquées sont présentées et exécutées de façon à conserver les jalons relatifs à la solution pilote, à la mise en œuvre progressive et à la stabilisation de la solution.

Question nº 155 :

Le changement 55 a remplacé le critère C4 par une autre exigence cotée totalement différente. TPSGC peut-il préciser le nombre de points total avec lequel le critère C4 sera évalué et la façon dont les points seront établis?

Réponse nº 155 :

L'évaluation technique C4 a été modifiée pour indiquer le calendrier des points demandé. Veuillez vous reporter au changement 89 de la présente modification.

Question nº 156 :

On dirait qu'il y a une erreur dans le tableau d'évaluation financière (échantillon). Le dénominateur des formules pour les soumissionnaires 1 et 2 semble être inversé.

Réponse nº 156 :

Le Canada confirme que les formules dans le tableau d'Exemple de sélection de soumission au point 4.4.1.9 de la partie de la DP sont exactes.

Question nº 157 :

En ce qui concerne la modification 004, changement 55, qui remplace la description originale du critère C4, plusieurs points nous préoccupent.

a) Quels que soient les scénarios opérationnels choisis, l'applicabilité à l'état final de la solution relative à Dynamics CRM et au portail demeurera peu concluante. En effet, il sera difficile de confirmer la réalité de ces scénarios jusqu'à ce que les parties de la restructuration des processus opérationnels concernant la réalisation de la solution soient effectuées. Les soumissionnaires sont déjà évalués d'après la restructuration des processus opérationnels dans d'autres parties de l'évaluation.

b) Ensuite, une variété de scénarios opérationnels de nombreux niveaux de complexité peuvent être sélectionnés. Il est donc possible que l'évaluation du critère C4 soit variable et subjective, ce qui rend difficile l'obtention d'une évaluation juste et équivalente parmi les divers soumissionnaires.

Les soumissionnaires doivent illustrer l'application des exigences en matière de sécurité pour l'évaluation et autorisation de sécurité ITSG-33 de TSSI et du gouvernement du Canada. La capacité des soumissionnaires serait donc plus juste si le critère C4 était remplacé par une exigence demandant de fournir un concept de sécurité indiquant les éléments suivants :

a) Une description de l'approche du soumissionnaire en matière de sécurité quant à la solution de TSSI de l'attribution du contrat jusqu'à la mise en service ainsi qu'au soutien que fournira le soumissionnaire à la solution de TSSI pendant son cycle d'évolution.

b) Une proposition de diagramme de topologie conforme à la sécurité ITSG-33/38 et des notes explicatives, qui tiennent compte que TSSI sera exploité dans un environnement d'hébergement conforme au GC et qui soulignent les dispositifs de sécurité convenables de la solution proposée, qui incluent notamment ce qui suit :

- Répartition des zones
- Cryptage
- Détection des intrusions
- Surveillance
- Contrôle d'accès
- Séparation des données
- Contrôle du flux de données

c) Une description narrative qui montre que le soumissionnaire comprend le processus de l'évaluation et de l'autorisation de sécurité ITSG-33, et qui explique son approche envers les activités principales pour chacune d'entre elles afin d'en assurer la réussite.

Nous demandons à l'État de réviser le critère C4 conformément à la description susmentionnée afin qu'elle examine les préoccupations le concernant. Toutefois, s'il décide de continuer avec l'approche des scénarios du critère C4 de la modification 004 révisée, on lui demande de déterminer les scénarios opérationnels en fournissant une description de trois scénarios; les soumissionnaires pourront choisir deux d'entre eux. Ainsi, il sera assuré que les soumissionnaires soumettent des scénarios de complexité similaire, qu'il sera possible d'évaluer de façon équivalente.

Remarque : L'observation ou recommandation soulignée à la question 87 peut être remplacée par la question 187 si SPAC peut confirmer ou clarifier que nous n'avons pas besoin de nous attaquer aux problèmes de sécurité de l'état opérationnel continu dans notre réponse concernant le critère C4 (autre que les détails compris à la question du critère C4).

Réponse nº 157 :

L'évaluation C4 originale diffère peu de la version révisée. Des exemples de scénarios opérationnels sont maintenant présentés, et les références à des contrôles de sécurité précis ont été modifiées pour mieux tenir compte d'une vaste portée de contrôles nécessaires.

En ce qui concerne l'évaluation technique C4, le soumissionnaire ne sera pas évalué sur les aspects de restructuration des processus opérationnels qui n'ont pas de lien avec la gestion de la sécurité ou d'autres aspects de sa réponse qui ne sont pas liés à la sécurité. L'objectif de l'évaluation C4 est d'évaluer la capacité des soumissionnaires à comprendre et à mettre en œuvre les exigences de sécurité nécessaires. Peu importe la complexité des scénarios choisis par l'entrepreneur, ce dernier doit présenter des réponses détaillées et pertinentes pour obtenir tous les points.

Question nº 158 :

Nous demandons à ce que la grille d'évaluation révisée pour le critère C4, qui comprend la note globale et la distribution de points pour chacun des sous-éléments de ladite grille, soit remise aux soumissionnaires.

Réponse nº 158 :

Veuillez consulter la réponse à la question 155 dans la présente modification 009.

Question nº 159 :

Pièce jointe 1 à la partie 4, O2, point E; modification 003, changement 40, 41 et 42; modification 004, réponse 38 – Le point E de O2 exige que l'un des projets de référence soit soumis aux mêmes exigences relatives à la sécurité que celles figurant à l'annexe A, section 5, 1.2, qui requièrent essentiellement que le projet respecte la ITSG-33 ou le NIST. Les changements 40, 41 et 42 de la modification 003 rehaussent les exigences relatives à l'intégrité du niveau moyen au niveau élevé, imposant ainsi d'autres restrictions au projet de référence.

Le Canada a reconnu (modification 004, R38) la possibilité qu'un nombre limité de projets gouvernementaux respectent O2; néanmoins, les exigences relatives à la sécurité requièrent presque assurément un projet gouvernemental afin de respecter les exigences relatives à la sécurité figurant à l'annexe A, section 5, 1.2.

Par nature, les contrôles de sécurité fonctionnent de la même façon, quelles que soient les données volumétriques, la diversité des transactions, etc.; or l'exigence selon laquelle un projet doit non seulement répondre aux exigences relatives à la sécurité, mais aussi à d'autres éléments du critère O2 est très restrictive.

Il est demandé que cette exigence soit modifiée afin de permettre au soumissionnaire de démontrer son expérience dans le cadre d'un projet (qui n'a pas à être l'un des trois projets appuyant le critère O2) pour lequel il a mis en œuvre des contrôles de sécurité semblables à ceux indiqués à l'annexe A, section 5, 1.2 – d'intégrité MOYENNE – afin de se conformer au point E du critère O2

Réponse nº 159 :

Le critère O2, élément E de l'évaluation technique a été retiré. Veuillez vous référer au changement 81 dans la modification 008.

Question nº 160 :

La modification 003 (changements 21 et 44) a donné lieu à une révision la LVERS afin d'indiquer que ce contrat est limité aux citoyens canadiens, y compris aux résidents permanents, car le fournisseur devra accéder à des renseignements ou à des biens INFOSEC. La partie 7, point 7.4 de la DP, comprend dorénavant une exigence d'évaluation de participation, contrôle et influence étrangers. Aux fins de la conformité à cette exigence obligatoire, le Canada pourrait-il fournir le questionnaire d'évaluation de PCIE afin que tous les soumissionnaires remplissent les formulaires dans les délais accordés.

Réponse nº 160 :

Le questionnaire PCIE est disponible comme pièce jointe à cette modification 009 comme référence. Veuillez noter que le questionnaire PCIE et toute documentation reliée à celle-ci ne doivent être soumis qu'après l'attribution du contrat.

Question nº 161 :

Modification 7, réponse à la question 106 :

L'État confirme que ***« le plan préliminaire de gestion du projet et le plan de gestion du projet*** sont exigés. Les critères A à F doivent être inclus comme composantes du plan de gestion du projet et ne sont pas des exigences distinctes ». L'État pourrait-il confirmer que seul le plan préliminaire de gestion du projet est exigé à la clôture des soumissions, et que le plan préliminaire de gestion du projet couvre les critères A à F de C1? En outre, l'État pourrait-il confirmer que le plan de gestion du projet sera élaboré durant la phase de planification et d'analyse du projet?

Réponse nº 161 :

L'État confirme qu'un plan préliminaire de gestion du projet sera conçu aux fins de l'évaluation des soumissions ainsi que pour alimenter le plan de gestion de projet réel de l'entrepreneur, qui doit être élaboré après l'attribution du contrat durant la phase de planification et d'analyse. L'État confirme également que le plan préliminaire de gestion du projet devrait contenir chaque élément énuméré au critère C1 de l'évaluation technique.

Question nº 162 :

Le changement 60, modification 6, indique ce qui suit :

« Le Portail Web de produits logiciels commerciaux est défini comme un ensemble de logiciels disponible sur le marché (en vente libre) qui fournit une composante d'échange vertical de données avec le public sur Internet (sur place) de la solution qui s'intègre à la plateforme de gestion des cas (sur place) et sert d'interface libre-service centrale et habilitante permettant les communications et les interactions entre les utilisateurs externes et les deux programmes du Secteur de la sécurité industrielle : le Programme de sécurité des contrats et le Programme des marchandises contrôlées. »

L'exigence susmentionnée se rapportant généralement à des projets de référence que les soumissionnaires doivent fournir, il est déraisonnable de les restreindre à des solutions qui prennent en charge les programmes du SSI de SPAC, comme tel est le cas actuellement. L'État pourrait-il supprimer la partie suivante du paragraphe susmentionné : « entre les utilisateurs externes et les deux programmes du Secteur de la sécurité industrielle : Programme de sécurité des contrats et le Programme des marchandises contrôlées »?

Réponse nº 162 :

Le Canada accepte et supprimera la formulation du paragraphe. Veuillez consulter le changement 90 dans la présente modification 009.

Question nº 163 :

La réponse à la question 106 concernant la modification 007 indique ce qui suit : « L'État a confirmé que le plan préliminaire de gestion du projet et le plan de gestion du projet sont exigés... ».

Le plan **préliminaire** de gestion du projet ne devrait-il pas être achevé durant l'étape d'identification de projet du SNGP avant la publication de la DP, afin de sélectionner un SI qui entreprendra l'étape de réalisation de projet, c.-à-d. que le plan préliminaire du projet (PPP) devrait déjà exister en tant qu'élément?

Nous recommandons que l'exigence du plan préliminaire de gestion du projet et du plan de gestion du projet soit remplacée dans C1 par ce qui suit : « Le soumissionnaire devrait fournir le plan de gestion du projet proposé... ».

Réponse nº 163 :

Veuillez prendre note que le Canada ne fait référence à aucun plan préliminaire de projet de SNGP dans cette exigence. Le Canada explique que le plan de gestion du projet proposé par les soumissionnaires dans cette évaluation est un « plan préliminaire de gestion du projet » du fait qu'un tel plan ne peut être élaboré qu'après l'attribution du contrat. Le plan préliminaire de gestion du projet sera uniquement utilisé aux fins de l'évaluation des soumissions. Le plan de gestion du projet sera le projet réel livrable en vertu du contrat. Veuillez consulter le changement 88 dans la présent modification 009.

TOUTES LES AUTRES MODALITÉS DEMEURENT INCHANGÉES.

Travaux publics et Services gouvernementaux Canada
Public Works and Government Services Canada

Participation, contrôle et influence étrangers

Lignes directrices à l'intention des organismes

Date de révision : le 10 avril 2014

Table des matières

PARTIE A – OBJECTIF D'UNE ÉVALUATION DE LA PARTICIPATION, DU CONTRÔLE ET DE L'INFLUENCE ÉTRANGERS

L'expression « participation, contrôle et influence étrangers » (PCIE) renvoie à une situation où l'on présume qu'un tiers étranger (personne, entreprise ou gouvernement) exerce une influence ou un contrôle suffisants sur une installation ou un organisme canadien pour pouvoir accéder, sans en avoir l'autorisation, à des renseignements classifiés.

Dans certaines situations qui ont trait à des programmes ou à des contrats visant à assurer la sécurité de renseignements de nature très délicate (INFOSEC), Services publics et Approvisionnement Canada (SPAC) doit effectuer une évaluation de la participation, du contrôle et de l'influence étrangers (évaluation de la PCIE) dont l'organisme fait l'objet ainsi qu'examiner le degré d'influence réelle ou potentielle des intérêts étrangers sur l'organisme. La réalisation d'une évaluation de la PCIE constitue aussi une exigence de la politique de sécurité de l'Organisation du Traité de l'Atlantique Nord (OTAN). Les pays membres de l'OTAN, y compris le Canada, doivent accorder une Attestation de sécurité d'installation (ASI) aux installations situées sur leur territoire qui sont utilisées pour des contrats mettant en jeu des renseignements classifiés de l'OTAN (de niveau confidentiel ou plus élevé)[1]. L'évaluation des facteurs de la PCIE fait partie de ce processus.

Lorsqu'un contrat nécessite une évaluation de la PCIE, l'organisme concerné doit notamment fournir au Secteur de la sécurité industrielle (SSI) de SPAC des renseignements sur la participation, sur l'influence et le contrôle étrangers possibles et réels ainsi que sur ses obligations et contrats à l'étranger. L'évaluation est effectuée par SPAC et entraîne une décision administrative quant à la nature et à la portée de l'influence étrangère sur la gestion ou les activités de l'organisme concerné.

La seule présence d'une participation, d'un contrôle ou d'une influence étrangers n'empêche pas un organisme d'obtenir une ASI. Les demandes sont évaluées au cas par cas. De plus, lorsque le SSI le juge nécessaire, un examen peut être effectué avec l'organisme afin de déterminer si certaines mesures peuvent être prises pour neutraliser le risque possible ou le réduire à un niveau acceptable.

L'évaluation du SSI mène à l'une des trois décisions suivantes : « Sans PCIE », « *Sans PCIE grâce à des mesures d'atténuation* » ou « Avec PCIE ».

PARTIE B – EXIGENCES RELATIVES AUX ÉVALUATIONS DE LA PCIE

L'évaluation de la PCIE est liée à l'obtention de l'ASI de l'organisme et doit être effectuée, entre autres, dans les cas suivants :

[1] La mention « classifié », dans le document, désigne les renseignements de niveau confidentiel ou plus élevé.

a. un organisme qui reçoit un contrat classifié de l'étranger ou de l'OTAN, ou encore un contrat INFOSEC doit faire l'objet d'une évaluation de la PCIE dans le cadre du processus d'obtention d'une ASI;
b. des modifications considérables ont été apportées aux renseignements concernant la PCIE précédemment fournis par l'organisme.

PARTIE C – LIGNES DIRECTRICES À L'INTENTION DES ORGANISMES

Les présentes lignes directrices ont pour but d'aider les organismes à préparer les documents nécessaires et à les soumettre à SPAC aux fins de l'évaluation de la PCIE. Veuillez les lire attentivement et respecter les directives à la lettre pour éviter les retards entraînés par une documentation sur la PCIE incomplète.

Directives spéciales :

1) Les documents soumis par les organismes sont considérés comme des déclarations d'entreprise juridiques certifiées devant contenir une description véridique et factuelle de leurs activités commerciales. Des questions laissées sans réponse, des documents justificatifs pertinents et requis qui manquent ou toute fausse déclaration (par omission, par dissimulation ou, encore, par des réponses trompeuses, fausses ou incomplètes) peuvent constituer des motifs pour refuser l'accès à du matériel INFOSEC ou à du matériel classifié de l'étranger ou de l'OTAN.

2) Si un organisme est dans l'impossibilité de fournir les documents demandés par le SSI, il doit fournir des documents de remplacement appropriés contenant les déclarations d'entreprise juridiques certifiées nécessaires, et expliquer la raison pour laquelle les documents demandés ne sont pas disponibles. Si aucun document de remplacement n'est disponible, le SSI procédera autrement pour obtenir les renseignements nécessaires, par exemple en demandant des renseignements supplémentaires à l'organisme, en interrogeant des cadres ou des dirigeants, en effectuant une visite des lieux, en faisant des vérifications d'antécédents et en ayant recours à divers autres procédés de vérification.

3) Une participation américaine doit être déclarée comme une participation étrangère. Dans le cadre de son évaluation, SPAC déterminera si cette participation est atténuée par d'autres facteurs ou si des mesures d'atténuation des risques sont nécessaires. Si l'organisme a déjà soumis la documentation relative à la PCIE aux États-Unis et qu'elle a été approuvée, cette documentation doit être jointe, de même que le formulaire d'attestation. SPAC tient compte de l'approbation des États-Unis dans le cadre du processus d'évaluation de la PCIE, mais cette approbation ne le remplace pas.

4) Une documentation sur la PCIE complète et distincte doit également être préparée et soumise pour l'organisme et pour chaque société mère, immédiate (directe) ou non (indirecte), de celui-ci. Il s'agit ici de réaliser les étapes 1, 2 et 3.

5) Tous les documents soumis doivent porter sur trois périodes distinctes : les deux derniers exercices financiers terminés et la période intermédiaire cumulative la plus récente de l'exercice courant.

On trouve un glossaire pertinent à la partie E.

Les documents seront conservés par le SSI et protégés conformément à la Politique sur la sécurité du gouvernement*, à l'annexe B de la* Norme opérationnelle sur la sécurité matérielle *et à l'annexe C de la* Directive sur la gestion de la sécurité ministérielle *du Secrétariat du Conseil du Trésor du Canada.*

Étape 1 – Répondre au questionnaire sur l'organisme

PROTÉGÉ une fois rempli

1) Il faut répondre à un questionnaire distinct pour l'organisme et pour chaque société mère, immédiate (directe) ou non (indirecte), de celui-ci.

QUESTION	NON	OUI	DANS L'AFFIRMATIVE, DANS QUELLE MESURE?	DANS L'AFFIRMATIVE, REPORTEZ-VOUS À L'ÉTAPE 3
1. Existe-t-il une participation étrangère ou des intérêts étrangers dans votre organisme?				
1.1. Est-ce que des intérêts étrangers détiennent, directement ou indirectement, des valeurs de votre organisme ou en ont la propriété effective?				Facteur nº 1.1
1.1. Est-ce que des intérêts étrangers contrôlent, influencent ou sont en mesure de contrôler ou d'influencer l'élection, la nomination ou la durée du mandat d'un des administrateurs ou dirigeants de votre organisme?				Facteur nº 1.2
1.1. Est-ce qu'une des catégories de valeurs ou de droits de propriété équivalents de votre organisme est enregistrée au nom d'un propriétaire apparent (prête-nom), ou selon une autre méthode qui ne permet pas de connaître l'identité du propriétaire effectif?				Facteur nº 1.3
2. Votre organisme détient-il, en totalité ou en partie, des intérêts étrangers?				Facteur nº 2
3. Est-ce qu'un intérêt étranger occupe un poste tel que celui d'administrateur ou de dirigeant au sein de votre organisme?				Facteur nº 3

4. Votre organisme tire-t-il un revenu d'intérêts étrangers ou de tout arrangement (contrat, accord, entente) avec des intérêts étrangers?				Facteurs n^{os} 4.1 et 4.2
5. Votre organisme a-t-il des dettes, des éléments de passif ou des obligations envers des intérêts étrangers?				Facteur n^{o} 5
6. Est-ce qu'un membre du conseil d'administration (ou d'une entité administrative similaire) de votre organisme occupe un poste ou est un consultant auprès d'intérêts étrangers?				Facteur n^{o} 6
7. Est-ce que des personnes, qu'il s'agisse d'employés ou non, qui peuvent se rendre à votre ou à vos installations à un titre quelconque, pourraient avoir accès à du matériel INFOSEC ou classifié de l'étranger ou de l'OTAN?				Facteur n^{o} 7
8. Votre organisme a-t-il une autre participation à l'étranger qui n'a pas été mentionnée dans vos réponses aux questions précédentes?				Facteur n^{o} 8

Tous les facteurs de PCIE mentionnés dans le présent questionnaire, qu'ils aient fait ou non l'objet d'une réponse positive, seront vérifiés ou confirmés par SPAC.

REMARQUES (joignez d'autres feuilles au besoin)

Étape 2 – Préparer les documents de base

1. Une documentation distincte doit être préparée et soumise pour l'organisme et pour chaque société mère, immédiate (directe) ou non (indirecte), de celui-ci.

2. Tous les documents soumis doivent porter sur les deux derniers exercices financiers terminés et sur la période intermédiaire cumulative la plus récente de l'exercice courant.

3. Les documents soumis doivent être classés selon un ordre séquentiel et explicitement marqués pour que le Secteur de la sécurité industrielle (SSI) puisse les étudier rapidement. En outre, on évitera ainsi de les renvoyer à l'organisme pour qu'il les mette à jour et y insère les renseignements manquants.

	Nom du dossier	**Commentaire ou précision (facultatif)**
1. Statuts et certificat de constitution		
2. Organigrammes		
a) Graphique de la participation dans l'organisme : ce graphique vise à déterminer le propriétaire ultime (société mère) et à présenter les titres détenus par chaque tiers faisant partie de l'« arbre généalogique » de l'organisme. Toutes les participations présentées dans le graphique doivent être exprimées en pourcentage (%) de la participation totale.		
b) Organigramme des conseils d'administration : l'organisme doit fournir la composition des conseils d'administration de toutes les sociétés de son « arbre généalogique », y compris le nom des membres, le titre de leur poste, leur citoyenneté et leur cote de sécurité, s'il y a lieu.		
3. Registre des procès-verbaux (ou tout autre document juridique tenu par le conseil d'administration conformément à la charte de l'organisme). S'il est impossible de présenter ce document en entier, on peut en présenter les extraits touchant directement la participation, le contrôle et l'influence étrangers ou des facteurs de PCIE précis.		
4. Registre des actionnaires		

5. Rapport annuel comprenant l'ensemble[2] des états financiers annuels vérifiés ainsi que le rapport connexe du vérificateur indépendant (dans le cas des sociétés ouvertes). Tous les états financiers annuels (vérifiés ou non ainsi que le rapport connexe du vérificateur indépendant, s'il y a lieu (dans le cas de sociétés fermées).		
6. Ensemble[1] des états financiers non vérifiés de la période intermédiaire cumulative la plus récente de l'exercice courant.		
7. Autres documents et renseignements pertinents. Il se peut que SPAC demande à l'organisme d'autres renseignements ou documents jugés pertinents dans le cadre de l'évaluation afin de rendre une décision appropriée. Il revient à l'organisme de fournir ces documents sur demande. Pour accélérer le processus, l'organisme peut décider de fournir tout document pertinent pouvant être utile avant qu'on le lui demande.		

[2] Par *ensemble*, on entend, au minimum : 1) le bilan (ou état de la situation financière); 2) le compte de résultat (ou état des résultats); 3) l'état des flux de trésorerie; 4) les notes afférentes aux états financiers, qui expliquent avec suffisamment de détails chacun des comptes importants, entre autres choses.

Étape 3 – Préparer les documents supplémentaires exigés pour chacun des facteurs

1. Chaque fois que vous avez répondu « Oui » à une question de l'étape 1, suivez les directives associées au facteur concerné et présenter les documents exigés. Cette étape doit être réalisée séparément, au besoin, par l'organisme et par chaque société mère, immédiate (directe) ou non (indirecte), de celui-ci qui a répondu au questionnaire.

2. Tous les documents soumis doivent porter sur les deux derniers exercices financiers terminés et sur la période intermédiaire cumulative la plus récente de l'exercice courant.

Facteur de PCIE nº 1

Participation ou participation effective étrangères

1.1

Participation ou participation véritable étrangères dans les valeurs ou les droits de propriété équivalents de l'organisme (1 % pour les sociétés fermées; 10 % pour les sociétés ouvertes).

1. Décrire la répartition générale de l'ensemble des actions et autres valeurs de l'organisme en pourcentage (%). Utiliser un graphique (diagramme à secteurs) qui illustre les différents liens, c'est-à-dire les administrateurs de l'organisme, les valeurs négociées sur le marché et la participation étrangère, etc.

2. Sous le graphique, décrire la répartition détaillée des actions et autres valeurs détenues à l'étranger et préciser les pourcentages de participation ainsi que le nom des personnes ou des organismes détenteurs, l'adresse des sièges sociaux de ces derniers et leur pays d'origine. Inclure ce qui suit :
    a. la participation indirecte par l'intermédiaire de filiales;
    b. les droits de vote associés à chaque catégorie d'actions.

3. Fournir une copie des conventions d'actionnaires, s'il y a lieu. Dans la négative, indiquer qu'il n'y a pas de convention d'actionnaires.

4. Les participations étrangères inférieures au seuil précisé (soit 1 % pour les sociétés fermées et 10 % pour les sociétés ouvertes) doivent être déclarées si elles permettent aux intérêts étrangers de contrôler ou d'influencer la nomination ou la durée du mandat des cadres supérieurs clés.

1.2

Intérêts étrangers qui contrôlent, qui influencent ou qui sont en mesure de contrôler ou d'influencer l'élection, la nomination ou la durée du mandat d'administrateurs ou de dirigeants de l'organisme, que ce pouvoir ait été exercé ou non.

Fournir le nom, la citoyenneté, l'adresse d'emploi et la cote de sécurité, le cas échéant, des intérêts étrangers, y compris tous les renseignements concernant le degré de participation dans les activités de l'organisme, de contrôle ou d'influence qu'ils peuvent exercer.

1.3

Un pour cent ou plus (sociétés fermées) et cinq pour cent ou plus (sociétés ouvertes) d'une catégorie des valeurs mobilières ou des droits de propriété équivalents de l'organisme qui sont enregistrés au nom d'un propriétaire apparent (prête-nom), ou selon une autre méthode qui ne permet pas de reconnaître l'identité du propriétaire effectif.

1. Donner le nom de chaque investisseur institutionnel étranger détenant, dans le cas d'un organisme fermé, au moins 1 % ou, dans le cas d'un organisme ouvert, au moins 5 % des actions donnant droit de vote. Donner le nom, l'adresse et le pourcentage d'actions détenues pour chaque personne ou organisme.

2. Pour chaque investisseur étranger, déclarer s'il a tenté d'exercer, ou a exercé, un contrôle de gestion ou une influence sur la nomination de cadres supérieurs clés, d'autres membres de la direction, ou encore sur les politiques de l'organisme. Donner des renseignements détaillés sur chacune de ces tentatives, sur les réponses de l'organisme ainsi que sur la situation actuelle.

3. Les valeurs *immatriculées au nom d'une maison de courtage* ou d'un établissement de placement doivent être comprises dans ce facteur. Le pourcentage d'actions *immatriculées au nom d'une maison de courtage* que détient chaque organisme doit être fourni.

Facteur de PCIE nº 2

Participation de l'organisme d'au moins 10 % dans des intérêts étrangers.

1. Fournir des renseignements détaillés sur toutes les participations étrangères (sociétés, filiales, sociétés affiliées) de l'organisme. Les en-têtes des colonnes doivent être les suivants : nom de l'organisme; adresse; pays; participation en % (de la participation totale); dirigeants de la société mère et postes à l'étranger (y compris le nom, le titre, la citoyenneté, la cote de sécurité, s'il y a lieu, et la mesure dans laquelle ces personnes participent aux activités des organismes canadiens et étrangers).

2. Si un employé est *représentant d'un intérêt étranger*, l'organisme doit faire une déclaration concernant l'accès de cette personne à des renseignements INFOSEC ou classifiés de l'étranger ou de l'OTAN en raison de son poste ou de son expertise.

3. Chaque employé de l'organisme qui est *représentant d'un intérêt étranger* et qui a une cote de sécurité ou est en voie d'en obtenir une doit faire une déclaration d'affiliations étrangères. Dans le cas d'un cadre supérieur clé (CSC), la déclaration doit faire l'objet d'une note dans le registre des procès-verbaux du conseil d'administration de l'organisme.

   Les organismes qu'une société canadienne possède à l'étranger sont considérés comme des organismes étrangers.

Facteur de PCIE nº 3

Postes de direction occupés par des intérêts étrangers, comme ceux d'administrateur et de dirigeant.

1. Fournir le nom, la citoyenneté, le lieu de travail, l'adresse du lieu de travail, le titre du poste ainsi que la cote de sécurité de toutes les personnes étrangères qui occupent un poste de direction dans l'organisme.

2. Joindre des photocopies des règlements administratifs ou des statuts qui comprennent les descriptions des postes concernés. Si ces renseignements se trouvent tous déjà dans l'organigramme demandé à l'étape 2 (documents de base), aucun autre renseignement n'est nécessaire.

Facteur de PCIE nº 4

Arrangements avec des intérêts étrangers et revenu tiré de ceux-ci.

4.1

Arrangements (contrats, conventions ou ententes) avec des intérêts étrangers.

1. Utiliser un tableau ou un autre moyen plus efficace pour fournir les données des six catégories qui suivent pour chacun des arrangements qui représente au moins 5 % du revenu total ou du résultat net de l'organisme : nom; adresse; pays; nature de l'arrangement (voir ci-dessous); montant du revenu tiré (préciser la devise) de cet arrangement et % du revenu de l'organisme que ce montant représente.

2. Préciser également, en ce qui concerne la nature de l'arrangement : le nom de l'autre partie; le type d'arrangement (contrat, convention ou entente); des renseignements sur

l'objet de l'arrangement, sur sa nature commerciale ou militaire; préciser s'il comprend l'usage de renseignements INFOSEC ou classifiés de l'étranger ou de l'OTAN.

3. L'organisme doit fournir une copie ou un résumé de l'arrangement si, au cours de l'évaluation de cette partie, SPAC n'est pas en mesure de déterminer la portée de l'arrangement, ou encore en fait la demande pour une raison quelconque.

4. Si des biens assujettis aux contrôles à l'exportation du Canada sont exportés par un organisme dans le cadre d'arrangements (contrats, conventions ou ententes), la conformité aux exigences de la licence d'exportation doit être démontrée.

5. Si l'organisme participe à un grand nombre d'arrangements commerciaux (ne relevant pas du domaine de la défense) visant l'octroi de licences, des brevets, des secrets commerciaux, des entreprises conjointes ou des ententes de transfert de technologies, mais que ces derniers ne représentent qu'un faible pourcentage du revenu brut de l'organisme et n'impliquent aucun renseignement INFOSEC ou classifié de l'étranger ou de l'OTAN, l'explication à fournir peut prendre la forme d'une courte déclaration générale portant sur ces éléments. Préciser le pourcentage du revenu brut que l'ensemble de ces arrangements représente.

4.2

Ensemble des revenus tirés d'intérêts étrangers.

1. Indiquer si votre organisme tire au moins 5 % de son revenu total ou de son résultat net (en dollars canadiens ou dans la devise utilisée dans les états financiers) d'un intérêt étranger donné.

2. Indiquer si votre organisme tire, dans l'ensemble, au moins 30 % de son revenu total ou de son résultat net (en dollars canadiens ou dans la devise utilisée dans les états financiers) de ses intérêts étrangers.

3. Fournir un tableau détaillé du revenu brut (en dollars canadiens ou dans la devise d'origine) ventilé par pays d'origine des payeurs, y compris les recettes provenant des entités indiquées aux questions 1 et 2 ci-dessus. Les données du tableau doivent correspondre à celles qui figurent dans les états financiers fournis.

4. Divulguer tout revenu (autre que le revenu abordé aux questions précédentes du facteur n^{o} 4.2) provenant d'autres sources étrangères, comme des dividendes de filiales étrangères, des redevances relatives à des accords sur des licences ou des brevets, des dividendes sur des actions étrangères, un revenu de placements étrangers ou un revenu de biens immobiliers à l'étranger (préciser la devise).

Facteur de PCIE nº 5

Dettes, éléments de passif ou obligations envers des intérêts étrangers.

1) Indiquer si votre organisme, à titre d'emprunteur, de bénéficiaire d'un cautionnement, de garant ou autrement, a des dettes, des éléments de passif ou des obligations envers des intérêts étrangers. Fournir des renseignements sur le montant de toute dette étrangère (préciser la devise); le type de dette; le nom et l'adresse de l'organisme auprès duquel la dette est contractée; la couverture bancaire utilisée, y compris les actions donnant droit de vote; toute condition ou clause restrictive, ainsi que l'incidence de la dette sur l'actif à court terme de l'organisme. Fournir une copie des ententes ou des extraits pertinents, notamment les procédures à suivre en cas de manquement.

2) Dans le cas de débentures convertibles, l'organisme doit fournir des données précises (les droits, les privilèges, les options de conversion, etc.).

3) Préciser si des paiements de remboursement de prêts ont été ou sont en souffrance.

4) Préciser si une entité ou une personne étrangères garantit des dettes, des éléments de passif ou des obligations envers la société ou exerce un contrôle ou de l'influence sur le financement des activités de la société.

5) Toutes les garanties fournies par une société mère pour le compte de ses filiales doivent être documentées de façon détaillée. Des renseignements doivent être fournis sur l'établissement financier qui participe aux prêts et l'objet de ces prêts.

6) Les conditions des conventions de prêt, comme le pouvoir de nommer des membres du conseil ou du personnel de la direction, doivent être déclarées, et des données particulières doivent être fournies.

7) Des renseignements sur les arrangements, les engagements ou les éventualités hors bilan avec des intérêts étrangers doivent être fournis (préciser la devise), le cas échéant.

8) Répondre à la question du facteur de PCIE nº 5 par l'affirmative si l'organisme a une dette auprès d'une entité canadienne exploitée ou contrôlée directement ou indirectement par des intérêts étrangers. Si cette donnée est inconnue, le préciser.

Facteur de PCIE nº 6

Administrateurs, dirigeants, cadres et cadres supérieurs de l'organisme qui occupent un poste ou qui sont consultants auprès d'intérêts étrangers.

1) Fournir le nom, les fonctions ou le titre (ou poste) détenu, la citoyenneté, la cote de sécurité ainsi que le nom et l'adresse de l'organisme étranger, y compris le pays d'origine, de tous les administrateurs, dirigeants, cadres et cadres supérieurs qui occupent un poste ou qui sont consultants auprès d'intérêts étrangers.

2) Dans le cas d'administrateurs, de dirigeants, de cadres et de cadres supérieurs qui assument des rôles communs imbriqués auprès de différents organismes en même temps, déclarer tous les organismes en cause ainsi que les renseignements demandés précédemment.

3) Fournir ces mêmes renseignements pour les filiales, en propriété exclusive ou non, situées dans un pays étranger.

Facteur de PCIE nº 7

Accès à du matériel INFOSEC ou à du matériel classifié de l'étranger ou de l'OTAN au sein d'un organisme.

1) Donner le nom, le titre du poste, la nationalité, la cote de sécurité et le type de participation de tous les employés ayant accès à du matériel INFOSEC ou classifié de l'étranger ou de l'OTAN.

2) Décrire les mesures de contrôle et les tests mis en place pour gérer les risques associés au fait que ces employés peuvent avoir accès à du matériel INFOSEC ou à du matériel classifié de l'étranger ou de l'OTAN. Inscrire la date d'entrée en vigueur de ces mesures de contrôle et la date à laquelle les tests ont été réalisés pour la dernière fois.

3) Préciser si l'organisme a été victime d'une infraction ou d'un incident relativement à du matériel INFOSEC ou classifié de l'étranger ou de l'OTAN au cours des dix dernières années, et décrire les mesures de contrôle internes supplémentaires mises en place pour prévenir, empêcher et repérer de telles infractions ou de tels incidents à l'avenir. Toutes ces infractions et tous ces incidents doivent être décrits en détail.

4) Préciser si l'organisme a fait une demande d'évaluation de la PCIE au cours des cinq dernières années auprès de membres de l'OTAN. Pour chaque demande d'évaluation de la PCIE acceptée, fournir une description générale des services rendus dans le cadre du contrat attribué, le nom du pays concerné, la durée du contrat ainsi que l'attestation de sécurité PCIE. Pour chaque demande d'évaluation refusée, indiquer en détail les raisons pour lesquelles le contrat n'a pas été accordé.

Facteur de PCIE nº 8

Autres facteurs qui laissent croire que des intérêts étrangers ont la possibilité de contrôler ou d'influencer la gestion ou les activités d'un organisme.

Fournir tout commentaire, observation, précision et renseignement pertinent relativement à la PCIE qui n'a pas été abordé dans les réponses précédentes (facteurs nº 1 à 7).

Étape 4 – Remplir le formulaire d'attestation et de consentement − PCIE

L'organisme doit soumettre un formulaire d'attestation et de consentement − PCIE dûment signé (partie F). Cette attestation constitue un document légal exigeant qu'un dirigeant de l'organisme atteste que tous les documents soumis à SPAC sont factuels, exacts, exhaustifs et exempts de toute inexactitude importante.

Avant de remplir le formulaire, s'assurer que tous les renseignements et les documents exigés ont été préparés et rassemblés selon les présentes lignes directrices. Tous les documents exigés dans le cadre de l'évaluation de la PCIE sont visés par cette attestation; le formulaire d'attestation ne doit être ni signé ni daté avant que tous les renseignements aient été recueillis et rassemblés.

Aucune documentation d'évaluation de la PCIE incomplète ne doit être attestée ni distribuée, car l'attestation serait alors considérée comme non valable et la documentation, renvoyée pour qu'y soient ajoutés les renseignements manquants.

Si, une fois le formulaire d'attestation rempli, SPAC découvre que les documents présentés sont frauduleux ou dénaturés, il peut s'agir d'un motif suffisant pour mettre fin au processus d'évaluation de la PCIE, et, par conséquent, empêcher toute participation de l'organisme à des contrats ou à des négociations dans le cadre desquels des renseignements INFOSEC ou classifiés de l'étranger ou de l'OTAN sont en jeu.

Étape 5 – Soumettre les documents

Une fois les étapes précédentes terminées, tous les documents exigés à la partie C (étapes 1 à 4) doivent être soumis électroniquement sur CD, DVD ou sur une clé USB. Les renseignements doivent être présentés de façon claire et concise, et les différents documents doivent être bien identifiés.

1. Questionnaire de l'organisation *(se reporter à l'étape 1)*.
2. Documents de base (points 1 à 7) *[se reporter à l'étape 2]*.
3. Documents supplémentaires exigés pour chaque facteur *(se reporter à l'étape 3)*. Préciser clairement les facteurs visés et classer les documents par facteur.
4. Formulaire d'attestation (PCIE) signé *(se reporter à l'étape 4)*.

Envoyer le CD, le DVD ou la clé USB à :

Secteur de la sécurité industrielle
Salle de courrier principale de SPAC
Place du Portage, Phase III, pièce 0B3
11, rue Laurier
Gatineau (Québec) K1A 0S5
À l'attention du : Bureau PCIE du SSI, 2745, rue Iris (6e étage)

Personne-ressource :

Envoyer vos questions par courriel à : SSI Évaluation PCIE — ISS FOCI Evaluation.

Étape 6 – Informer SPAC des changements organisationnels (continu)

Si des changements ayant une incidence sur l'information transmise au SSI se produisent dans les activités commerciales d'un organisme, il incombe à l'organisme de les signaler au SSI le plus tôt possible.

> **Important : si ces changements touchent directement la participation, le contrôle et l'influence étrangers, le Secteur de la sécurité industrielle doit être avisé par écrit immédiatement.**

PARTIE D – ÉVALUATION DE SPAC ET RÉSULTATS

Après avoir reçu les documents, SPAC effectuera une évaluation afin de déterminer la nature et la portée de l'influence étrangère sur la gestion ou les activités de l'organisme. Le Centre de la sécurité des télécommunications Canada (CSTC) est pour sa part responsable d'approuver la divulgation de renseignements INFOSEC à des organismes non gouvernementaux. SPAC doit donc faire approuver par le CSTC les résultats de l'évaluation de la PCIE lorsque des renseignements INFOSEC sont en jeu.

À la suite de l'évaluation, le SSI attribue à l'organisme l'une des désignations suivantes :

- Sans PCIE
- Avec PCIE – aucune mesure d'atténuation nécessaire
    - Le SSI attribuera cette désignation à l'organisme dans le cas où il relève des facteurs courants atténuant les risques.
- Avec PCIE – mesures d'atténuation nécessaires
    - Le SSI déterminera si l'organisme peut appliquer des mesures d'atténuation des risques relevés. Dans un tel cas, le SSI communiquera d'autres directives à l'organisation.
- Avec PCIE – aucune mesure d'atténuation possible
    - Dans un tel cas, l'organisme n'aura pas le droit de participer à des contrats INFOSEC ni à des contrats classifiés de l'étranger ou de l'OTAN.

PARTIE E – GLOSSAIRE

Accord : entente ayant force de loi conclue entre au moins deux parties ayant la capacité juridique de le faire. Les accords ou contrats peuvent porter sur les fiducies ayant droit de vote, les licences, les ventes, les brevets, les secrets commerciaux, le transfert de technologies, les agences, la formation de cartels, les sociétés de personnes, les coentreprises, etc.

Propriétaire effectif : personne qui a les droits d'un actionnaire même si son nom n'apparaît pas sur le certificat d'actions ou ne se trouve pas dans le registre des actionnaires. Il peut s'agir d'une personne qui détient une participation par l'intermédiaire d'un fiduciaire, d'un représentant légal, d'un agent, d'un mandataire ou d'un autre intermédiaire.

Obligation (*bond*) : titre de créance par lequel un investisseur prête des fonds à une entité (société ou organisme gouvernemental) pour une période définie à un taux d'intérêt fixe.

Cartel : organisme créé à la suite d'une entente officielle conclue entre un groupe de producteurs d'un bien ou d'un service en vue d'en réguler l'offre, afin de contrôler ou de manipuler les prix.

Sécurité des communications électroniques (COMSEC) : protection résultant de l'application de mesures de sécurité cryptographique, de sécurité de la transmission et de sécurité des émissions aux télécommunications, aux émissions ne provenant pas de télécommunications et au matériel d'acheminement des données, de même que de l'application d'autres mesures pertinentes aux renseignements et au matériel visés par la COMSEC. La COMSEC comprend également les directives relatives à la réalisation de cette protection. Ces mesures sont destinées à empêcher que ne soit compromise l'intégrité des renseignements stockés sur des systèmes informatiques ou transmis ou traités par ceux-ci. La COMSEC garantit également l'authenticité des télécommunications.

Sécurité des systèmes informatiques (COMPUSEC) : protection résultant de l'application de mesures conçues pour empêcher que ne soit compromise l'intégrité des renseignements stockés sur un système informatique ou traités par celui-ci. Cette protection découle de l'application, aux installations informatiques, de mesures de sécurité relativement au matériel informatique, aux logiciels et aux opérations, ainsi que d'autres mesures appropriées aux systèmes et aux installations informatiques, sauf la COMSEC.

Débenture convertible : obligation que le détenteur peut échanger contre une action donnant droit de vote.

Covenant : entente officielle conclue entre au moins deux parties et obligeant celles-ci à faire ou à ne pas faire quelque chose. Un covenant négatif ou restrictif interdit au promettant de s'engager dans certaines activités, tandis qu'un covenant positif ou affirmatif oblige le promettant à respecter certaines exigences. Un covenant ayant trait aux obligations est une

modalité juridiquement contraignante d'une entente entre l'émetteur d'une obligation et l'obligataire, visant à protéger les intérêts des deux parties.

Débenture : billet ou obligation garantis par la réputation de crédit de son émetteur.

Titre de créance : une obligation, une débenture ou un autre titre visant une dette ou une garantie d'une société, que ce titre soit garanti ou non.

Administrateur : personne physique nommée par les actionnaires d'une société pour superviser la gestion de la société. Ensemble, les directeurs d'une société par actions forment un « conseil d'administration ».

Attestation de sécurité d'installation : décision administrative confirmant que l'organisme peut, sur le plan de la sécurité, avoir accès à des renseignements ou des biens « classifiés » ou « protégés » appartenant à un niveau de classification identique ou inférieur à celui de l'attestation délivrée.

Intérêt étranger : tout gouvernement étranger, tout organisme d'un gouvernement étranger, toute forme d'entreprise organisée conformément aux lois d'un pays autre que le Canada, toute forme d'entreprise organisée ou constituée selon les lois du Canada ou d'une province canadienne qui est exploitée ou contrôlée par un gouvernement étranger, une société étrangère ou une personne de l'étranger. Cette définition comprend toute personne physique n'ayant ni la citoyenneté ni la nationalité canadienne.

Participation, contrôle ou influence étrangers : situation où un tiers étranger (personne, entreprise ou gouvernement) est présumé exercer une influence ou un contrôle suffisants sur un organisme ou une installation canadiens pour pouvoir accéder, sans en avoir l'autorisation, à des renseignements classifiés de l'étranger ou de l'OTAN ou à des renseignements INFOSEC.

Dette : chose due à un tiers ou obligation envers un tiers.

Sécurité de l'information (INFOSEC) : tous les renseignements et les documents COMSEC ou COMPUSEC confiés au Centre de la sécurité des télécommunications ou élaborés et évalués par celui-ci ou pour celui-ci.

- **Contrat INFOSEC** : tout contrat, contrat de sous-traitance, négociation précontractuelle ou autre convention ou entente approuvés par le gouvernement impliquant la divulgation de renseignements INFOSEC ou la participation à un programme d'évaluation de produits INFOSEC du Centre de la sécurité des télécommunications.
- **Matériel INFOSEC** : matériel, y compris les programmes informatiques ou autres données, conçu pour assurer la sécurité des systèmes de télécommunications et des systèmes informatiques.

Coentreprise : contrat de société ou entente de coopération entre plusieurs personnes ou sociétés généralement engagées dans une seule entreprise. De manière générale, la coentreprise est de courte durée et peut viser, par exemple, la conception et la construction d'un bâtiment ou d'une structure.

Cadre supérieur clé : personne devant obtenir une attestation de sécurité avant que son organisme puisse obtenir une Attestation de sécurité d'installation. Sont compris dans cette catégorie l'agent de sécurité d'entreprise ainsi que les propriétaires, les dirigeants, les administrateurs, les cadres et les partenaires qui occupent un poste où il est possible de nuire aux politiques et aux pratiques de l'organisme lors de l'exécution de contrats classifiés.

Obligation (*liability*) : terme juridique possédant un sens large. En règle générale, ce terme renvoie à une dette active. Il s'agit de l'état d'être de fait ou potentiellement lié par une obligation; de l'état d'être responsable d'une éventuelle perte ou d'une perte réelle, d'un dédit, d'un acte répréhensible, d'une dépense ou de coûts indirects; d'un état qui engendre l'obligation d'agir immédiatement ou à l'avenir.

Licence conventionnelle : entente écrite signée par le propriétaire d'un bien ou d'une activité et donnant la permission à un tiers d'utiliser ce bien ou de s'engager dans une activité relative à ce bien. Le bien visé par une licence conventionnelle peut être un bien réel ou personnel, ou il peut s'agir de propriété intellectuelle.

Action d'un prête-nom : action pour laquelle le nom inscrit sur le certificat d'enregistrement n'est pas celui du détenteur réel.

Organisation du Traité de l'Atlantique Nord (OTAN) : alliance de 28 pays d'Amérique du Nord et d'Europe résolus à réaliser les objectifs du Traité de l'Atlantique Nord de 1949. Le rôle essentiel de l'OTAN est de sauvegarder la liberté et la sécurité de ses pays membres. La participation du Canada à l'OTAN facilite l'échange de renseignements avec les pays membres lorsqu'une exigence en matière de sécurité industrielle se présente.

Obligation (*obligation*) : accord obligeant à verser de l'argent ou une autre contrepartie d'importance.

Hors bilan : actif, dette ou activité de financement qui n'apparaît pas sur le bilan d'un organisme.

Dirigeant : personne physique nommée par les administrateurs d'une société pour gérer les activités quotidiennes de celle-ci, comme le président, le vice-président, le secrétaire, le trésorier, le contrôleur, l'avocat général, le directeur général, un administrateur délégué ou toute autre personne qui remplit pour une société des fonctions semblables à celles remplies par les personnes qui occupent ces postes. Le poste de dirigeant est distinct de celui d'administrateur, bien qu'il soit fréquent qu'une même personne occupe les deux postes dans une petite société.

Organisme : personne ou entité autres qu'un ministère, un organisme ou une société d'État du gouvernement fédéral canadien. Cela comprend les sociétés ou entités commerciales, les facultés universitaires et les sociétés de personnes.

Représentant d'intérêts étrangers : citoyen du Canada agissant à titre de représentant, de dirigeant, d'agent ou d'employé pour un gouvernement étranger, une entreprise étrangère, une

société étrangère ou une personne de l'étranger. Cependant, une personne ayant la citoyenneté ou la nationalité canadienne qui a été nommée par son employeur canadien pour le représenter dans la gestion d'une filiale étrangère (c.-à-d. une entreprise étrangère dans laquelle la société canadienne a une participation dans au moins 51 % des actions donnant droit de vote) ne sera pas considérée comme un représentant d'intérêts étrangers uniquement en raison de son emploi, à condition que cet employeur soit son employeur principal et que l'entreprise possède une Attestation de sécurité d'installation (ASI) ou soit en voie d'en obtenir une.

Valeur : action faisant partie de toute catégorie ou série d'actions ou titre de créance d'une société comprenant un certificat qui authentifie une telle action ou un tel titre de créance, c.-à-d. billet, action, obligation d'État, obligation, débenture, certificat d'intérêt, participation dans une convention de participation aux bénéfices, etc.

Immatriculation au nom d'une maison de courtage : pratique courante qui consiste à enregistrer des valeurs négociées sur le marché au nom d'une ou de plusieurs maisons de courtage de valeurs.

Transfert de technologies : entente conclue entre deux parties pour l'échange ou le transfert de technologies aux fins d'utilisation à l'interne ou de vente.

Convention de fiducie : entente selon laquelle une partie neutre, un fiduciaire, accepte d'assumer la responsabilité des actions donnant droit de vote et de gérer l'organisme d'une seconde partie, sans que cette seconde partie fasse obstruction.

PARTIE F – ATTESTATION ET CONSENTEMENT DE L'ORGANISME — PROPRIÉTÉ, CONTRÔLE ET INFLUENCE ÉTRANGERS

PROTÉGÉ une fois rempli

J'atteste avoir lu et compris cette confirmation que, à ma connaissance, les déclarations et renseignements transmis à Services publics et Approvisionnement Canada (SPAC) aux fins de l'évaluation de la propriété, du contrôle et de l'influence étrangers de l'organisme (nommé ci-dessous) ont été fournis de bonne foi et sont véridiques, complets et exacts, et que j'ai l'autorisation d'en certifier la véracité au nom de l'organisme.

Je consens à la divulgation des renseignements soumis par l'organisme aux fins d'une vérification ultérieure ou d'une enquête pour la tenue d'une évaluation de la propriété, du contrôle et de l'influence étrangers en vue d'obtenir une Attestation de sécurité d'installation (ASI). Je reconnais que ces renseignements peuvent également être vérifiés ou utilisés dans le cadre d'une enquête lorsque l'ASI fait l'objet d'une mise à jour ou de tout autre examen pour les raisons prévues dans la Politique sur la sécurité du gouvernement (PGS). Je reconnais que les renseignements recueillis peuvent être divulgués à la Gendarmerie royale du Canada (GRC), au Service canadien du renseignement de sécurité (SCRS) ou à d'autres ministères ou organismes aux fins de vérifications ou d'enquêtes, conformément à la PGS. Mon consentement demeurera valide jusqu'à ce qu'une ASI ne soit plus nécessaire, ou jusqu'à ce qu'un administrateur autorisé de cet organisme envoie un avis par écrit au Secteur de la sécurité industrielle (SSI) de SPAC pour la révoquer.

_____ _____

Nom Signature

_____ _____

Titre Organisme

_____

Date