RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Title - Sujet Système de contrôle d'accès	
Solicitation No. - N° de l'invitation 0D160-204228/A	**Date** 2020-06-16
Client Reference No. - N° de référence du client 0D160-204228	
GETS Reference No. - N° de référence de SEAG PW-$$HN-329-78815	
File No. - N° de dossier hn329.0D160-204228	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-07-28**	**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: Dumaresq, Steve	**Buyer Id - Id de l'acheteur** hn329
Telephone No. - N° de téléphone (613) 296-1704 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See Herein	

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée See Herein	**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**	

Issuing Office - Bureau de distribution

Electrical & Electronics Products Division
L'Esplanade Laurier
East Tower, 4th floor,
Ottawa
Ontario
K1A 0S5

PRÉSENTATION DES SOUMISSIONS

Compte tenu de la pandémie actuelle de COVID 19, il est recommandé que tous les fournisseurs soumettent leur soumission par le service Connexion postel:
Puisque plusieurs personnes travaillent présentement de la maison et dans le but de prévenir la propagation de la maladie à coronavirus (COVID-19) dans les communautés, les soumissionnaires sont fortement encouragés à utiliser le service Connexion postel pour la transmission électronique de leur soumission.

Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.

Remarque : Pour les soumissionnaires qui choisissent de présenter leurs soumissions en utilisant Connexion postel pour la clôture des soumissions à l'Unité de réception des soumissions dans la région de la capitale nationale, l'adresse de courriel est la suivante :

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Remarque : Les soumissions ne seront pas acceptées si elles sont envoyées directement à cette adresse de courriel. Cette adresse de courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'indiqué dans les instructions uniformisées 2003 ou pour envoyer des soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

- - -

Si vous rencontrez des difficultés avec le système de connexion postel, vous pouvez contacter notre unité de réception des soumissions à l'adresse suivante pour obtenir de l'aide:

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

N'envoyez pas une soumission ou offre directement à cette adresse.

VISITES DU SITE NON DISPONIBLE

Compte tenu de la situation du COVID-19, les restrictions imposées par le gouvernement aux exigences de rassemblements publics et exigences en matière de distance physique, limitent la capacité d'effectuer des visites traditionnelles des lieux. En raison de ses besoins immédiats, Sécurité publique Canada a décidé de distribuer des renseignements détaillés sur ses systèmes actuels aux soumissionnaires intéressés à la suite de la signature d'une entente de non-divulgation. Une téléconférence aura lieu, en remplacement des visites traditionnel, où toutes les questions seront répondu.

SPÉCIFICATIONS DISPONIBLES SUR CLÉ USB

Les soumissionnaires intéressés doivent envoyer un courriel à l'autorité contractante pour demander une copie des spécifications qui ont été mises à disposition.

Le soumissionnaire doit inclure une annexe G, Accord de non-divulgation pour la sollicitation et le contrat, avec la demande de spécifications pour chaque personne qui y aura accès.

Steve Dumaresq
Travaux publics et Services gouvernementaux Canada
Direction générale des approvisionnements
Direction du transport et des produits logistiques, électriques et pétroliers - Division HN

steve.dumaresq@tpsgc-pwgsc.gc.ca

Remarque: Une clé USB sera envoyée par service de messagerie. Fournissez l'adresse complète et les coordonnées.

CONFÉRENCE DES SOUMISSIONNAIRES (TÉLÉCONFÉRENCE)

Date, heure et détails de la conférence des soumissionnaires (téléconférence) seront fournis lors de l'acceptation de la demande du soumissionnaire pour les spécifications sur clé USB.

Dans le cadre de la conférence, on examinera la portée du besoin précisé dans la demande de soumissions et on répondra aux questions qui seront posées. Il est recommandé que les soumissionnaires qui ont l'intention de déposer une soumission assistent à la conférence.

Ils devraient fournir à l'autorité contractante, par écrit, une liste des personnes qui assisteront à la conférence.

Toute précision ou tout changement apporté à la demande de soumissions à la suite de la conférence des soumissionnaires sera inclus dans la demande de soumissions, sous la forme d'une modification. Les soumissionnaires qui ne participeront pas à la conférence pourront tout de même présenter une soumission.

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La demande de soumissions et de contrat subséquent compte sept parties ainsi que des annexes comme suit:

Partie 1 Renseignements généraux : renferme une description générale du besoin;

Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, clauses et conditions relatives à la demande de soumissions;

Partie 3 Instructions pour la préparation des soumissions : donne aux soumissionnaires les instructions pour préparer leurs soumissions;

Partie 4 Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, s'il y a lieu, ainsi que la méthode de sélection;

Partie 5 Attestations : comprend les attestations à fournir;

Partie 6 Clauses du contrat subséquent: contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

Les annexes comprennent l'énoncé des spécifications techniques, la base de paiement, les exigences en matière de sécurité, l'attestation du Programme de contrats fédéraux pour l'équité en matière d'emploi, les exigences en matière d'assurances et toutes autres annexes.

1.2 Résumé

1.2.1 L'administration centrale de Sécurité publique/Public Safety Canada (SPPS) dans la région de la capitale nationale doit actuellement mettre à niveau son ancien système de contrôle d'accès et des intrusions.

Les exigences initiales concernent deux (2) emplacements à Ottawa, Ontario: 269 Laurier et 340 Laurier. Le contrat comprendra l'option de futures mises à niveau et installations du système à divers endroits au Canada.

Le travail comprend la conception, la fourniture, l'installation, l'essai et la formation technique du Système de sécurité intégrée d'entreprise (SSIE) tel que décrit dans l'énoncé des spécifications techniques (EST). Se référer à l'annexe A.

1.2.2 Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples renseignements, veuillez consulter la Partie 6, Clauses du contrat subséquent.

1.2.3 Ce besoin est assujetti aux dispositions de l'Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP–OMC), de l'Accord de libre-échange nord-américain (ALENA), de l'Accord économique et commercial global entre le Canada et l'Union européenne (AECG) et de l'Accord de libre-échange canadien (ALEC).

1.3 Compte rendu

Après l'attribution du contrat, les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Les soumissionnaires devraient en faire la demande à l'autorité contractante dans les 15 jours ouvrables, suivant la réception des résultats du processus de demande de soumissions. Le compte rendu peut être fourni par écrit, par téléphone ou en personne.

PARTIE 2 - INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites dans le *Guide des clauses et conditions uniformisées d'achat* (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Travaux publics et Services gouvernementaux Canada.

Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

Le document 2003 (2020-05-28) Instructions uniformisées - biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

Le paragraphe 5.4 du document 2003, Instructions uniformisées – biens ou services – besoins concurrentiels, est modifié comme suit :

Supprimer : 60 jours
Insérer : 120 jours

2.2 Présentation des soumissions

Compte tenu de la pandémie actuelle de COVID 19, il est recommandé que tous les fournisseurs soumettent leur soumission par le service Connexion postel:
Puisque plusieurs personnes travaillent présentement de la maison et dans le but de prévenir la propagation de la maladie à coronavirus (COVID-19) dans les communautés, les soumissionnaires sont fortement encouragés à utiliser le service Connexion postel pour la transmission électronique de leur soumission.

Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.

Remarque : Pour les soumissionnaires qui choisissent de présenter leurs soumissions en utilisant Connexion postel pour la clôture des soumissions à l'Unité de réception des soumissions dans la région de la capitale nationale, l'adresse de courriel est la suivante :

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Remarque : Les soumissions ne seront pas acceptées si elles sont envoyées directement à cette adresse de courriel. Cette adresse de courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'indiqué dans les instructions uniformisées 2003 ou pour envoyer des soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

2.3 Demandes de renseignements – en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins dix (10) jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

Les soumissionnaires devraient citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le

Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les soumissionnaires.

2.4 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur en Ontario, et les relations entre les parties seront déterminées par ces lois. À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées.

2.5 Améliorations apportées aux besoins pendant la demande de soumissions

Les soumissionnaires qui estiment qu'ils peuvent améliorer, techniquement ou technologiquement, le devis descriptif ou l'énoncé des travaux contenus dans la demande de soumissions, sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer clairement les améliorations suggérées et les motifs qui les justifient. Les suggestions, qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier, seront examinées à la condition qu'elles parviennent à l'autorité contractante au plus tard quatorze (14) jours avant la date de clôture de la demande de soumissions. Le Canada aura le droit d'accepter ou de rejeter n'importe quelle ou la totalité des suggestions proposées.

PARTIE 3 - INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1. Instruction pour la préparation des soumissions

- Si le soumissionnaire choisit d'envoyer sa soumission par voie électronique, le Canada exige de sa part qu'il respecte l'article 08 des instructions uniformisées 2003. Le système Connexion postel a une limite de 1 Go par message individuel affiché et une limite de 20 Go par conversation.

  La soumission doit être présentée en sections distinctes comme suit :

  Section I : Soumission technique
  Section II : Soumission financière
  Section V : Attestations
  Section VI : Renseignements supplémentaires

- Si le soumissionnaire choisit de transmettre sa soumission sur papier, le Canada demande que la soumission soit présentée en sections distinctes, comme suit :

  Section I : Soumission technique (2 copies papier) et 2 copies électroniques sur clés USB;
  Section II: Soumission financière (1 copie papier) et 1 copie électronique sur clé USB;
  Section V : Attestations (1 copie papier) et 1 copie électronique sur clé USB;
  Section VI : Renseignements supplémentaires (1 copie papier) et 1 copie électronique sur clé USB.

  En cas d'incompatibilité entre le libellé de la copie électronique sur le media et de la copie papier, le libellé de la copie papier l'emportera sur celui de la copie électronique.

- Si le soumissionnaire fournit simultanément plusieurs copies de sa soumission à l'aide de méthodes de livraison acceptable, et en cas d'incompatibilité entre le libellé de la copie électronique transmise par le

service Connexion postel et celui de la copie papier, le libellé de la copie électronique transmise par le service Connexion postel aura préséance sur le libellé des autres copies.

- Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué dans une autre section de la soumission.

Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué dans une autre section de la soumission.

Le Canada demande que les soumissionnaires suivent les instructions de présentation décrites ci-après pour préparer leur soumission.

a) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm);
b) utiliser un système de numérotation correspondant à celui de la demande de soumissions:

En avril 2006, le Canada a approuvé une politique exigeant que les agences et ministères fédéraux prennent les mesures nécessaires pour incorporer les facteurs environnementaux dans le processus d'approvisionnement Politique d'achats écologiques (http://www.tpsgc-pwgsc.gc.ca/ ecologisation-greening/achats-procurement/politique-policy-fra.html). Pour aider le Canada à atteindre ses objectifs, on encourage les soumissionnaires à:

1) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm) contenant des fibres certifiées provenant d'un aménagement forestier durable et/ou contenant au moins 30 % de matières recyclées; et

2) utiliser un format qui respecte l'environnement : impression noir et blanc, recto-verso/à double face, broché ou agrafé, sans reliure Cerlox, reliure à attaches ni reliure à anneaux.

Section I : Soumission technique

Dans leur soumission technique, les soumissionnaires devraient démontrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Les soumissionnaires devraient démontrer leur capacité et décrire l'approche qu'ils prendront de façon complète, concise et claire pour effectuer les travaux.

La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

Section II : Soumission financière

Les soumissionnaires doivent présenter leur soumission financière en conformité avec toutes les exigences en matière de prix présentées dans le présent document.

3.1.1 Fluctuation du taux de change – Atténuation des risques

1. Le soumissionnaire peut demander au Canada d'assumer les risques et les avantages liés aux fluctuations du taux de change. Si le soumissionnaire demande un rajustement du taux de change, cette demande doit être clairement indiquée dans la soumission au moment de sa présentation. Le soumissionnaire doit présenter le formulaire PWGSC-TPSGC 450, Demande de rajustement du taux de change, avec sa soumission, et indiquer le montant en monnaie étrangère en dollars canadiens pour chaque article pour lequel un rajustement du taux de change est demandé.
2. Le montant en monnaie étrangère est défini comme la portion du prix ou du taux qui varie directement en fonction des fluctuations du taux de change. Ce montant devrait comprendre l'ensemble des taxes, des droits et des autres coûts payés par le soumissionnaire et qui seront compris dans le montant de rajustement.
3. Le prix total payé par le Canada sur chaque facture sera rajusté au moment du paiement, selon le montant en monnaie étrangère et la disposition relative à la fluctuation du taux de change du contrat. Le rajustement du taux de change sera uniquement appliqué lorsque la fluctuation du taux de change varie de plus de 2% (augmentation ou diminution).
4. Au moment de la soumission, le soumissionnaire doit remplir les colonnes (1) à (4) du formulaire PWGSC-TPSGC 450 pour chaque article pour lequel il veut se prévaloir de la disposition relative à la fluctuation du taux de change. Lorsque les soumissions sont évaluées en dollars canadiens, les valeurs indiquées dans la colonne (3) devraient aussi être en dollars canadiens, afin que le montant du rajustement soit présenté dans la même devise que le paiement.
5. Aux fins de la présente disposition relative à la fluctuation du taux de change, les autres taux ou calculs proposés par le soumissionnaire ne seront pas acceptés.

Section III: Attestations

Les soumissionnaires doivent présenter les attestations exigées à la Partie 5.

Les attestations que les soumissionnaires remettent au Canada peuvent faire l'objet d'une vérification à tout moment par le Canada. Le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur, s'il est établi qu'une attestation du soumissionnaire est fausse, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat.

Section IV : Renseignements supplémentaires

3.1.2 Représentant de l'entrepreneur

Nom et numéro de téléphone de la personne avec qui communiquer :

Renseignements généraux		**Suivi de la livraison**	
Nom :	_____	Nom :	_____
Téléphone :	_____	Téléphone :	_____
Télécopieur :	_____	Télécopieur :	_____
Courriel :	_____	Courriel :	_____

3.1.3 Réparations sous garantie

Il pourrait se révéler nécessaire d'effectuer sur les lieux des réparations sous garantie. On vous demande d'indiquer votre délai d'intervention et les coordonnées du bureau ou du dépôt le plus proche dans lequel des employés pourront effectuer ces travaux. Voici le nom de la personne à contacter:

Temps de réponse: _____
Nom : _____
No de téléphone : _____
No de télécopieur : _____
Adresse électronique : _____

3.1.4 Services et réparation d'urgence

À la demande de Service correctionnel Canada, l'entrepreneur devra assurer, pendant la durée du contrat, sur les lieux des services ou des réparations d'urgence qui ne font pas l'objet des dispositions relatives à la garantie des Conditions générales 2030. On paiera l'équipe d'urgence selon les modalités indiquées dans les présentes. Voici le nom de la personne à contacter:

Nom : _____
No de téléphone : _____
No de télécopieur : _____
Adresse électronique : _____

PARTIE 4 - PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

Pour le seul processus d'évaluation, le terme « **soumissionnaire** » désigne la personne ou l'entité (ou dans le cas d'une coentreprise, les personnes ou les entités) qui dépose une soumission pour l'exécution d'un contrat de biens, de services ou les deux. Le terme peut également inclure la société mère ou les filiales du soumissionnaire.

4.1 Procédures d'évaluation

(a) Les soumissions reçues seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation techniques, de gestion, du soutien et financiers mentionnés ci-bas.

(b) Une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.

4.1.1 Évaluation technique

La soumission technique, de gestion et de soutien devraient être concis et traiter, sans nécessairement s'y limiter, des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée.

Les soumissionnaires devraient traiter de ces critères d'évaluation de manière suffisamment approfondie dans leur soumission. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Les soumissionnaires devraient expliquer et démontrer comment ils entendent répondre aux exigences et comment ils réaliseront les travaux.

Il est rappelé au soumissionnaire de fournir autant d'informations et de documents techniques que possible, afin de démontrer pleinement la conformité technique à tous les éléments de la demande de soumissions, sinon la proposition peut être jugée non conforme (non recevable) pour insuffisance d'informations.

4.1.1.1 Critères techniques obligatoires

Simplement indiquer qu'un critère est respecté n'est pas suffisant. Les soumissionnaires doivent présenter une soumission bien organisée et imprimée (pas manuscrite) qui comprend toutes les informations techniques et descriptives requises pour démontrer la conformité à chacun des critères présentés dans l'Énoncé des spécifications techniques (EST) à l'Annexe A, ainsi que toutes autres caractéristiques ci-incluses.

Deux (2) sites initiaux: 269 Laurier (Ottawa) et 340 Laurier (Ottawa)

Pour chaque site :
a) Conformité à toutes les exigences présentées dans cette demande de soumissions;
b) Conformité technique à l'énoncé des exigences à l'annexe A;
c) Conformité technique aux critères obligatoires présentées à l'annexe B;
d) Le soumissionnaire doit soumettre une solution de sécurité complète pour chaque site avec toute l'information et documentation nécessaire pour démontrer la conformité au besoin présenté dans cette demande.

Les soumissions seront évaluées sous la base de réussite/échec. Les soumissions qui ne sont pas conformes à tous les critères obligatoires seront jugées non-recevables et aucune autre considération ne leur sera portée.

4.1.1.2 Critères techniques cotés

a) Conformité technique aux critères techniques cotés à l'annexe B;
b) 5 points seront attribués pour chaque année supplémentaire d'expérience de projet de taille et de portée similaires (après 5 ans d'expérience obligatoire identifié à M1). (15 points max.).

4.1.2 Évaluation financière

Conformité à toutes les exigences financières présentées dans cette demande de soumissions;
Conformité et achèvement du barème de prix à l'annexe C.

4.1.2.1 Base de prix

Le soumissionnaire doit fournir des prix fermes, en dollars canadiens, rendu droits acquittés (Ottawa, Ontario). Les frais de transport à destination doivent être inclus ainsi que les droits de douane et la taxe d'accise applicable. Taxes de ventes TVH/TPS non inclus.

Si le soumissionnaire demande la protection contre les fluctuations du taux de change, un formulaire de demande d'ajustement du taux de change (PWGSC-TPSGC 450) dûment rempli doit être inclus dans la soumission présentée.

4.1.3 Méthode de sélection - le prix le plus bas par point

Pour être déclarée recevable, une soumission doit :

a. respecter toutes les exigences de la demande de soumissions; et
b. satisfaire à tous les critères d'évaluation techniques obligatoires.

Les soumissions ne répondant pas aux exigences de a) ou b) seront déclarées non recevables. La soumission recevable ayant obtenu le plus de points ou celle ayant le prix le plus bas ne sera pas nécessairement acceptée.

La soumission recevable ayant le prix le plus bas par point sera recommandée pour attribution d'un contrat.
Prix le plus bas par point = Offre totale évaluée $ (site 1+ site 2) / Nombre de points évalués obtenus (max. 15).

PARTIE 5 – ATTESTATIONS

Les soumissionnaires doivent fournir les attestations et la documentation exigées pour qu'un contrat leur soit attribué.

Les attestations que les soumissionnaires remettent au Canada peuvent faire l'objet d'une vérification à tout moment par le Canada. Le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur, s'il est établi qu'une attestation du soumissionnaire est fausse, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat.

L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. À défaut de répondre à cette demande, la soumission sera également déclarée non recevable, ou sera considéré comme un manquement au contrat.

5.1 Attestations obligatoires exigées avec la soumission

Les soumissionnaires doivent fournir les attestations suivantes dûment remplies avec leur soumission.

5.1.1 Déclaration de condamnation à une infraction

Conformément au paragraphe Déclaration de condamnation à une infraction de l'article 01 des instructions uniformisées, le soumissionnaire doit, selon le cas, présenter avec sa soumission le Formulaire de déclaration (http://www.tpsgc-pwgsc.gc.ca/ci-if/formulaire-form-fra.html) dûment rempli afin que sa soumission ne soit pas rejetée du processus d'approvisionnement.

5.1.2 Statut et disponibilité du personnel

Le soumissionnaire atteste que, s'il obtient le contrat découlant de la demande de soumissions, chaque individu proposé dans sa soumission sera disponible pour exécuter les travaux, tel qu'exigé par les représentants du Canada, au moment indiqué dans la demande de soumissions ou convenue avec ce dernier. Si pour des raisons hors de son contrôle, le soumissionnaire est incapable de fournir les services d'un individu identifié dans sa soumission, le soumissionnaire peut proposer un remplaçant avec des qualités et une expérience similaire. Le soumissionnaire doit aviser l'autorité contractante de la raison pour le remplacement et fournir le nom, les qualités et l'expérience du remplaçant proposé. Pour les fins de cette clause, seule les raisons suivantes seront considérées comme étant hors du contrôle du soumissionnaire : la mort, la maladie, la retraite, la démission, le congédiement justifié ou la résiliation par manquement d'une entente.

Si le soumissionnaire a proposé un individu qui n'est pas un employé du soumissionnaire, le soumissionnaire il atteste qu'il a la permission de l'individu d'offrir ses services pour l'exécution des travaux et de soumettre son curriculum vitae au Canada. Le soumissionnaire doit, sur demande de l'autorité contractante, fournir une confirmation écrite, signée par l'individu, de la permission donnée au soumissionnaire ainsi que de sa disponibilité. Le défaut de répondre à la demande pourrait avoir pour conséquence que la soumission soit déclarée non recevable.

_____ _____

Signature ***Date***

5.1.3 Études et expérience

Le soumissionnaire atteste qu'il a vérifié tous les renseignements fournis dans les curriculum vitae et les documents à l'appui présentés avec sa soumission, plus particulièrement les renseignements relatifs aux études, aux réalisations, à l'expérience et aux antécédents professionnels, et que ceux-ci sont exacts. En outre, le soumissionnaire garantit que les chaque individu qu'il a préposé est en mesure d'exécuter les travaux prévus dans le contrat éventuel.

_____ _____

Signature ***Date***

5.2 Attestations préalables à l'attribution du contrat et renseignements supplémentaires

Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être remplis et fournis avec la soumission mais ils peuvent être fournis plus tard. Si l'une de ces attestations ou renseignements supplémentaires ne sont pas remplis et fournis tel que demandé, l'autorité contractante informera le soumissionnaire du délai à l'intérieur duquel les renseignements doivent être fournis. À défaut de fournir les attestations ou les renseignements supplémentaires énumérés ci-dessous dans le délai prévu, la soumission sera déclarée non recevable.

5.2.1 Dispositions relatives à l'intégrité – liste de noms

Les soumissionnaires constitués en personne morale, y compris ceux qui présentent une soumission à titre de coentreprise, doivent transmettre une liste complète des noms de tous les administrateurs.

Les soumissionnaires qui présentent une soumission en tant que propriétaire unique, incluant ceux présentant une soumission comme coentreprise, doivent fournir le nom du ou des propriétaire(s).

Les soumissionnaires qui présentent une soumission à titre de société, d'entreprise ou d'association de personnes n'ont pas à soumettre une liste de noms.

5.2.2 Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation de soumission

En présentant une soumission, le soumissionnaire atteste que le soumissionnaire, et tout membre de la coentreprise si le soumissionnaire est une coentreprise, n'est pas nommé dans la liste des « soumissionnaires à admissibilité limitée » (http://www.travail.gc.ca/fra/normes_equite/eq/emp/pcf/liste/inelig.shtml) du Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi disponible sur le site Web d'Emploi et Développement social Canada (EDSC) – Travail.
Le Canada aura le droit de déclarer une soumission non recevable si le soumissionnaire, ou tout membre de la coentreprise si le soumissionnaire est une coentreprise, figure dans la liste des « soumissionnaires à admissibilité limitée » du PCF au moment de l'attribution du contrat.

5.2.3 Attestation des caractéristiques environnementales générales

Le soumissionnaire doit sélectionner et remplir l'une des deux déclarations suivantes aux fins d'attestation

A) Le soumissionnaire atteste que le soumissionnaire est inscrit ou rencontre la norme ISO 14001.

_____ _____

Signature du représentant autorisé du soumissionnaire **Date**

OU

B) Le soumissionnaire atteste que le soumissionnaire satisfait et continuera de satisfaire, pendant toute la durée du contrat, à un minimum de quatre (4) des six (6) critères identifiés dans le tableau ci-dessous.

Le soumissionnaire doit indiquer qu'il satisfait à un minimum de quatre (4) critères.

Pratiques écologiques au sein de l'organisation des soumissionnaires	**Insérez un crochet pour chaque critère qui est respecté.**
Favorise un environnement sans papier au moyen de directives, procédures et / ou programmes.	
Tous les documents sont imprimés recto verso et en noir et blanc dans le cadre des activités quotidiennes, excepté lors d'indications contraires par votre client.	
Le papier utilisé dans le cadre des activités quotidiennes est composé d'un minimum de 30% de matières recyclées et possède une certification de la gestion durable des forêts.	
Utilise préférablement des encres écologiques et achète des cartouches d'encre réusinées ou cartouches d'encre qui peuvent être retournées au fabricant aux fins de réutilisation et de recyclage dans le cadre des activités quotidiennes.	
Des bacs de recyclage pour le papier, le papier journal, le plastique et l'aluminium sont disponibles et vidés régulièrement conformément au programme de recyclage local.	
Un minimum de 50% de matériel de bureau détient une certification écoénergétique.	

_____ _____

Signature du représentant autorisé du soumissionnaire **Date**

PARTIE 6 - CLAUSES DU CONTRAT SUBSÉQUENT

Les clauses et conditions suivantes s'appliquent à tout contrat subséquent découlant de la demande de soumissions et en font partie intégrante.

1. Exigences relatives à la sécurité

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau **protégé**, délivrées par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC)
2. Ce contrat comprend un accès à des marchandises contrôlées. Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées (PMC) de TPSGC
3. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens protégés, ou à des établissements de travail dont l'accès est réglementé, doivent tous détenir une cote de **fiabilité** en vigueur, délivrée ou approuvée par la DSIC/TPSGC
4. L'entrepreneur ne doit pas utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données et(ou) de production au niveau protégé tant que la DSIC/TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées jusqu'au niveau **protégé**
5. Les contrats de sous-traitance comportant des exigences relatives à la sécurité ne doivent pas être attribués sans l'autorisation écrite préalable de la DSIC/TPSGC
6. L'entrepreneur ou l'offrant doit se conformer aux dispositions des documents suivants :
    1. de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe
    2. le Manuel de la sécurité industrielle (dernière édition)

2. Énoncé du besoin

L'entrepreneur doit concevoir, fournir, installer et mettre à l'essai les solutions de sécurité tel que décrit dans l'énoncé des spécifications techniques et documentation connexes, tel que présenté dans cette demande de soumissions.

2.1 Exigence initial

Deux (2) sites : 269 Laurier (Ottawa) et 340 Laurier (Ottawa)

2.2 Exigence optionnel – Expansion future

La nature et l'étendue exactes des travaux pour les besoins des bureaux régionaux seront déterminées ultérieurement, lorsque les besoins et les lieux seront connus. D'autres sites peuvent inclure, mais sans s'y limiter: Burnaby (C.-B.), Edmonton (AB), Regina (SK), Winnipeg (MB), Fredericton (N.-B), Toronto (ON), Ottawa (ON), Montreal (QC), Dartmouth (N.-E), Charlottetown (I-P-E), St. John's (TN).

3. Autorisation de tâches

La totalité ou une partie des travaux du contrat seront réalisés sur demande, au moyen d'une autorisation de tâches (AT). Les travaux décrits dans l'AT doivent être conformes à la portée du contrat

3.1 Processus d'autorisation des tâches

1. Le responsable technique fournira à l'entrepreneur une description des tâches au moyen du « Formulaire d'autorisation des tâches» tel que spécifié comme annexe au contrat.

2. L'AT comprendra les détails des activités à exécuter, une description des produits à livrer et un calendrier indiquant les dates d'achèvement des activités principales ou les dates de livraison des produits livrables. L'AT comprendra également les bases et les méthodes de paiement applicables, comme le précise le contrat.
3. Dans les 14 jours civils suivant la réception de l'AT, l'entrepreneur doit fournir au responsable technique le coût total estimatif proposé pour l'exécution des tâches et une ventilation de ce coût, établie conformément à la Base de paiement du contrat.
4. L'entrepreneur ne doit pas commencer les travaux avant la réception de l'AT autorisée par le responsable technique. L'entrepreneur reconnaît qu'avant la réception d'une AT le travail effectué sera à ses propres risques.

3.2 Limite d'autorisation de tâches

Toutes les autorisations de tâches doivent être approuvées par l'autorité contractante avant d'être émises.

3.3 Rapports périodiques d'utilisation - Contrats avec autorisation de tâches

L'entrepreneur doit compiler et tenir à jour des données sur les services fournis au gouvernement fédéral, conformément à l'autorisation de tâches approuvée émise dans le cadre du contrat.

L'entrepreneur doit fournir ces données conformément aux exigences d'établissement de rapports précisées ci-dessous. Si certaines données ne sont pas disponibles, la raison doit en être indiquée. Si aucun service n'a été fourni pendant une période donnée, l'entrepreneur doit soumettre un rapport portant la mention « néant ».

Les données doivent être présentées tous les trimestres à l'autorité contractante.

Voici la répartition des trimestres :
Premier trimestre : du 1er avril au 30 juin;
Deuxième trimestre : du 1er juillet au 30 septembre;
Troisième trimestre : du 1er octobre au 31 décembre; et
Quatrième trimestre : du 1er janvier au 31 mars.

Les données doivent être présentées à l'autorité contractante dans les dix (10) jours civils suivant la fin de la période de référence.

Exigence en matière de rapport - Explications
Il faut tenir à jour un dossier détaillé de toutes les tâches approuvées pour chaque contrat avec une autorisation de tâches (AT). Le dossier doit comprendre :

Pour chaque AT autorisée:
i. le numéro de la tâche autorisée ou le numéro de révision de la tâche;
ii. le titre ou une courte description de chaque tâche autorisée;
iii. le coût estimatif total précisé dans l'AT autorisée de chaque tâche, excluant les taxes applicables;
iv. le montant total, excluant les taxes applicables, dépensé jusqu'à maintenant pour chaque AT autorisée;
v. dates de début et de fin de chaque AT autorisée;
vi. l'état actuel de chaque AT autorisée, (s'il y a lieu).

Pour toutes les AT autorisées:
i. Le montant (excluant les taxes applicables) précisé dans le contrat (selon la dernière modification, s'il y a lieu) de la responsabilité totale du Canada envers l'entrepreneur pour toutes les AT autorisées;
ii. le montant total, excluant les taxes applicables, dépensé jusqu'à présent pour toutes les AT autorisées.

4. Clauses et conditions uniformisées

Toutes les clauses et conditions identifiées dans le contrat par un numéro, une date et un titre, sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (CCUA) https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat publié par Travaux publics et Services gouvernementaux Canada.

4.1 Conditions générales

2030 (2020-05-28) Conditions générales - besoins plus complexes de biens.

4.2 Conditions générales supplémentaires

4001 (2015-04-01) Achat, location et maintenance de matériel;
4003 (2010-08-16) Logiciels sous licence;
4004 (2013-04-25) Services de maintenance et de soutien des logiciels sous licence; et

4.3 Clauses du guide des CCUA

B1501C (2018-06-21)	Appareillage électrique
A9068C (2010-01-11)	Emplacement - règlements
A2000C (2006-06-16)	Ressortissants étrangers (entrepreneur canadien)
A2001C (2006-06-16)	Ressortissants étrangers (entrepreneur étranger)

5. Durée du contrat

5.1 Période du contrat

La période du contrat est pour trois (3) an, donc du __date__ au __date__ inclusivement.

5.2 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus deux (2) périodes supplémentaires de d'une (1) année chacune, selon les mêmes conditions. L'entrepreneur accepte que pendant la période prolongée du contrat, il sera payé conformément aux dispositions applicables prévues à la Base de paiement.

Période d'option un (1) : Du __date__ au __date__ inclusivement;
Période d'option deux (2) : Du __date__ au __date__ inclusivement.

Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur avant la date d'expiration du contrat. Cette option ne pourra être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

6. Responsables

6.1 Autorité contractante

Steve Dumaresq
Travaux publics et Services gouvernementaux Canada
Direction générale des approvisionnements
Direction du transport et des produits logistiques, électriques et pétroliers - Division HN
L'Esplanade Laurier, 140 rue O'Connor, Tour Est
Téléphone : (613) 296-1704
Courriel : steve.dumaresq@tpsgc-pwgsc.gc.ca

L'autorité contractante est responsable de la gestion du contrat, et toute modification doit être autorisée, par écrit par l'autorité contractante. L'entrepreneur ne doit pas effectuer de travaux dépassant la portée du contrat ou des travaux qui n'y sont pas prévus suite à des demandes ou des instructions verbales ou écrites de toute personne autre que l'autorité contractante.

6.2 Responsable technique

Nom :
Titre :
Téléphone : (xxx) xxx-xxxx
Télécopieur : (xxx) xxx-xxxx
Courriel :

Le responsable technique représente le ministère ou organisme pour lequel les travaux sont exécutés dans le cadre du contrat. Il est responsable de toutes les questions liées au contenu technique des travaux prévus dans le contrat. On peut discuter des questions techniques avec le responsable technique; cependant, celui-ci ne peut pas autoriser les changements à apporter à l'énoncé des travaux. Ces changements peuvent être effectués uniquement au moyen d'une modification au contrat émise par l'autorité contractante.

6.3 Représentant de l'entrepreneur

Renseignements généraux
Nom : ____
Téléphone : ____
Télécopieur : ____
Courriel : ____

Suivi de la livraison
Nom : _____
Téléphone : _____
Télécopieur : _____
Courriel : _____

6.4 Réparations sous garantie

Le nom de la personne à contacter s'il se révèle nécessaire d'effectuer sur les lieux des réparations sous garantie.

Temps réponse : _____
Nom: _____
Numéro de téléphone : _____
Numéro de télécopieur: _____
Courriel : _____

6.5 Services et réparation d'urgence

À la demande de l'Agence des services frontaliers du Canada, l'entrepreneur devra assurer, pendant la durée du contrat, sur les lieux des services ou des réparations d'urgence qui ne font pas l'objet des dispositions relatives à la garantie des Conditions générales 2030. On paiera l'équipe d'urgence selon les modalités indiquées dans les présentes. Voici le nom de la personne à contacter:

Nom: _____
Numéro de téléphone : _____
Numéro de télécopieur: _____
Courriel : _____

7. Paiement

7.1 Base de paiement

L'Entrepreneur sera payé les prix de lot fermes pour l'équipement, l'installation et le test, des frais de déplacement, la formation sur place, comme - des dessins construits et des manuels comme spécifié dans le Contrat. Les droits de douane sont inclus et les taxes sont en sus, le cas échéant.

L'Entrepreneur sera payé un taux horaire fixe pour toutes les heures travaillées sous chaque catégorie de travail indiquée pour l'installation et évaluant sur normal et à l'extérieur des heures de travail associées aux réparations d'urgence, des retards, conçoit des changements et des surgissements de travail non prévus.

Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

7.1.1 Autorisation de tâches

L'entrepreneur sera remboursé pour les coûts qu'il a engagés raisonnablement et convenablement dans l'exécution des travaux décrits dans l'autorisation de tâches (AT) approuvée, comme ils ont été déterminés conformément à la base de paiement qui figure à l'annexe B, jusqu'à la limite des dépenses indiquée dans l'AT approuvée.

La responsabilité du Canada envers l'entrepreneur en vertu de l'AT approuvée ne doit pas dépasser la limitation des dépenses indiquée dans l'AT approuvée. Les droits de douane sont inclus et les taxes applicables sont en sus.

Aucune augmentation de la responsabilité totale du Canada ou du prix des travaux précisés dans toute AT approuvée découlant de tout changement à la conception, ou de toute modification ou interprétation des travaux, ne sera autorisée ou payée à l'entrepreneur, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés, par écrit, par l'autorité contractante avant d'être intégrés aux travaux.

7.1.2 Déplacement pour effectuer des travaux liés à une autorisation de tâches

L'entrepreneur sera remboursé pour ses frais autorisés de déplacement et de subsistance qu'il a raisonnablement et convenablement engagés dans l'exécution des travaux, au prix coûtant, sans aucune indemnité pour le profit et(ou) les frais administratifs généraux, conformément aux indemnités relatives aux repas, à l'utilisation d'un véhicule privé et aux faux frais qui sont précisées aux appendices B, C et D de la Directive sur les voyages du *Conseil national mixte* et selon les autres dispositions de la Directive qui se rapportent aux « voyageurs » plutôt que celles qui se rapportent aux « employés »

Tout voyage doit recevoir l'autorisation préalable de l'autorité technique. Tous les paiements sont assujettis à une vérification des comptes par le gouvernement.

7.2 Limite de prix

Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

7.3 Limite des dépenses – Total cumulatif de toutes les autorisations de tâches

1. La responsabilité totale du Canada envers l'entrepreneur dans le cadre du contrat pour toutes les autorisations de tâches autorisées, y compris toutes révisions, ne doit pas dépasser la somme de __$. Les droits de douane et les taxes applicables sont inclus.

2. Aucune augmentation de la responsabilité totale du Canada ne sera autorisée ou payée à l'entrepreneur, à moins qu'une augmentation ait été approuvée, par écrit, par l'autorité contractante.

3. L'entrepreneur doit informer, par écrit, l'autorité contractante concernant la suffisance de cette somme :

    a. lorsque 75 p. 100 de la somme est engagée, ou

    b. quatre (4) mois avant la date d'expiration du contrat, ou

    c. dès que l'entrepreneur juge que la somme est insuffisante pour l'achèvement des travaux requis dans le cadre des autorisations de tâches, y compris toutes révisions,
    selon la première de ces conditions à se présenter.

4. Lorsqu'il informe l'autorité contractante que les fonds du contrat sont insuffisants, l'entrepreneur doit lui fournir par écrit une estimation des fonds additionnels requis. La présentation de cette information par l'entrepreneur n'augmente pas la responsabilité du Canada à son égard.

7.4 Vérification discrétionnaire

L'attestation de l'entrepreneur à l'effet que le prix ou taux indiqué n'est pas supérieur au plus bas prix ou taux demandé à toute personne, y compris au meilleur client de l'entrepreneur, pour des biens, services ou les deux de qualité et de quantité semblables, peut faire l'objet d'une vérification des comptes par le gouvernement, à la discrétion du Canada, avant ou après que l'entrepreneur n'ait été payé.

Si la vérification des comptes démontre que l'attestation est erronée après que le paiement ait été versé à l'entrepreneur, ce dernier doit, à la discrétion du Canada, rembourser au Canada le montant qui est supérieur au plus bas prix ou taux ou autoriser le Canada à retenir le montant en le déduisant de toute somme payable à l'entrepreneur en vertu du contrat.

Si la vérification des comptes démontre que l'attestation est erronée avant que le paiement ne soit effectué, l'entrepreneur convient que le Canada ajustera les factures en suspens, en fonction des résultats de la vérification. En outre, il est entendu que si le contrat est toujours en vigueur au moment de la vérification, le prix ou taux sera réduit en fonction des résultats de la vérification des comptes.

7.5 Contrôle du temps

Le temps facturé et l'exactitude du système d'enregistrement du temps de l'entrepreneur peuvent faire l'objet d'une vérification par le Canada, avant ou après que l'entrepreneur ait été payé. Si la vérification est effectuée après le paiement, l'entrepreneur devra rembourser, à la demande du Canada, tout paiement en trop.

7.6 Paiement mensuel

Clause H1008C (2008-05-12) Paiement mensuel

7.7 Instructions relatives à la facturation

1. L'entrepreneur doit soumettre ses factures conformément à l'article intitulé « Présentation des factures » des conditions générales.

2. En soumettant les factures, l'entrepreneur certifie que les biens et services ont été livrés et que tous les frais sont conformes à la base de paiement du contrat, y compris les frais pour les travaux effectués par des sous-traitants.

7.8 Frais de déplacement de subsistance

L'entrepreneur sera remboursé pour ses frais autorisés de déplacement et de subsistance qu'il a raisonnablement et convenablement engagés dans l'exécution des travaux, au prix coûtant, sans aucune indemnité pour le profit et(ou) les frais administratifs généraux, conformément aux indemnités relatives aux repas, à l'utilisation d'un véhicule privé et aux faux frais qui sont précisées aux appendices B, C et D de la Directive sur les voyages du *Conseil national mixte* et selon les autres dispositions de la Directive qui se rapportent aux « voyageurs » plutôt que celles qui se rapportent aux « employés »

Tout voyage doit recevoir l'autorisation préalable de l'autorité technique.
Tous les paiements sont assujettis à une vérification par le gouvernement.

8. Attestations - Conformité

Le respect continu des attestations fournies par l'entrepreneur avec sa soumission ainsi que la coopération constante quant aux renseignements supplémentaires sont des conditions du contrat. Les attestations pourront faire l'objet de vérifications par le Canada pendant toute la durée du contrat. En cas de manquement à toute déclaration de la part de l'entrepreneur ou à fournir les renseignements supplémentaires, ou encore si on constate que les attestations qu'il a fournies avec sa soumission comprennent de fausses déclarations, faites sciemment ou non, le Canada aura le droit de résilier le contrat pour manquement conformément aux dispositions du contrat en la matière.

9. Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur en Ontario et les relations entre les parties seront déterminées par ces lois.

10. Ordre de priorité des documents

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste.

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste.

(a) les articles de la convention;
(b) les conditions générales supplémentaires :
  (i) 4001 (2015-04-01) Achat, location et maintenance de matériel;
  (ii) 4003 (2010-08-16), Logiciels sous licence;
  (iii) 4004 (2013-08-16) Services de maintenance et de soutien des logiciels sous licence; et
(c) les conditions générales 2030 (2020-05-28), Conditions générales - besoins plus complexes de biens;
(d) Annexe __, Énoncé des spécifications technique;

(e) Annexe __, Prix et Base de paiement;
(f) les autorisations de tâches signées et incluant les annexes;
(g) Annexe __, Liste de vérification des exigences relatives à la sécurité;
(h) la soumission de l'entrepreneur en date du __.

11. Assurances

L'entrepreneur est responsable de décider s'il doit s'assurer pour remplir ses obligations en vertu du contrat et pour se conformer aux lois applicables. Toute assurance souscrite ou maintenue par l'entrepreneur est à sa charge ainsi que pour son bénéfice et sa protection. Elle ne dégage pas l'entrepreneur de sa responsabilité en vertu du contrat, ni ne la diminue.

12. Divulgation des renseignements

L'entrepreneur devra garder confidentiels et ne devra ni publier, ni réutiliser, diffuser, divulguer ou communiquer à des tiers les renseignements originaux ou de base se rapportant au dessins des systèmes installés, aux dessins des établissements et aux manuels, sauf dans les cas qui pourront être jugés nécessaires pour permettre d'exécuter les travaux en vertu du contrat; dans ces cas, l'entrepreneur devra imposer la même obligation de confidentialité à toutes les personnes auxquelles l'information sera divulguée.

ANNEXE A ÉNONCÉ DES EXIGENCES
ANNEXE B CRITÈRES D'ÉVALUATION TECHNIQUE

ANNEXE C PRIX ET BASE DE PAIEMENT

PARTIE 1 SOLUTIONS DE SÉCURITÉ POUR 269 LAURIER (OTTAWA) ET 340 LAURIER (OTTAWA)

SITE UN : 269 LAURIER (OTTAWA)

Le soumissionnaire doit fournir des prix fermes, en dollars canadiens, rendu droits acquittés (Ottawa, Ontario). Les frais de transport à destination doivent être inclus ainsi que les droits de douane et la taxe d'accise applicable. Les frais de déplacement et de subsistance doivent être inclus. Taxes de ventes TVH/TPS non inclus.

Si le soumissionnaire demande la protection contre les fluctuations du taux de change, un formulaire de demande d'ajustement du taux de change (PWGSC-TPSGC 450) dûment rempli doit être inclus dans la soumission présentée.

Prix de lot - Répartition des coûts
Avant l'adjudication du contrat, le soumissionnaire doit fournir une répartition ligne par ligne de tous les prix indiqués dans l'annexe C – Prix et Base de Paiement. Les prix fournis serviront à calculer le coût des autorisations de tâches pendant toute la durée du contrat.

SOLUTION PROPOSÉE PAR L'ENTREPRENEUR pour 269 Laurier (Ottawa)

1. CONCEPTION DU SYSTÈME

Prix de lot ferme pour la conception.

CONCEPTION	***PRIX DE LOT:_____ $***

2. LIVRAISON DE L'ÉQUIPEMENT

Prix de lot ferme pour tout l'équipement connexe, excluant les pièces de rechange.

ÉQUIPEMENT	***PRIX DE LOT:_____ $***

3. INSTALLATION ET FRAIS DE DÉPLACEMENT CONNEXES

Le prix doit comprendre tous les coûts, y compris les dépenses de déplacement et de subsistances, liés à l'installation.

INSTALLATION	***PRIX DE LOT:_____ $***

4. INTÉGRATION ET MISE À L'ESSAI DU LOGICIEL

INTÉGRATION DU LOGICIEL	***PRIX DE LOT:_____ $***
FRAIS DE MISE À L'ESSAI	***PRIX DE LOT:_____ $***

5. FORMATION SUR PLACE ET DOCUMENTATION

COÛT DE LA FORMATION SUR PLACE	***PRIX DE LOT:_____ $***

DESSINS CONFORMES À L'EXÉCUTION DES TRAVAUX	***PRIX DE LOT: _____ $***

MANUELS	***PRIX DE LOT: _____ $***

6. CONTRAT DE SERVICE POUR LE SUPPORT ET LA MAINTENANCE

CONTRAT DE SERVICE	**Prix – 1 année**
Conformément à l'annexe A	$

SOLUTION PROPOSÉE DE L'ENTREPRENEUR pour 269 Laurier (Ottawa)	***PRIX TOTAL DE LA SOUMISSION : _____$*** ***Somme des articles 1 à 6 ci-haut***

ANNEXE C PRIX ET BASE DE PAIEMENT (suite)

SITE DEUX : 340 LAURIER (OTTAWA)

Le soumissionnaire doit fournir des prix fermes, en dollars canadiens, rendu droits acquittés (Ottawa, Ontario). Les frais de transport à destination doivent être inclus ainsi que les droits de douane et la taxe d'accise applicable. Les frais de déplacement et de subsistance doivent être inclus. Taxes de ventes TVH/TPS non inclus.

Si le soumissionnaire demande la protection contre les fluctuations du taux de change, un formulaire de demande d'ajustement du taux de change (PWGSC-TPSGC 450) dûment rempli doit être inclus dans la soumission présentée.

Prix de lot - Répartition des coûts
Avant l'adjudication du contrat, le soumissionnaire doit fournir une répartition ligne par ligne de tous les prix indiqués dans l'annexe C – Prix et Base de Paiement. Les prix fournis serviront à calculer le coût des autorisations de tâches pendant toute la durée du contrat.

SOLUTION PROPOSÉE PAR L'ENTREPRENEUR pour 340 Laurier (Ottawa)

1. CONCEPTION DU SYSTÈME

Prix de lot ferme pour la conception.

CONCEPTION	***PRIX DE LOT:_____ $***

2. LIVRAISON DE L'ÉQUIPEMENT

Prix de lot ferme pour tout l'équipement connexe, excluant les pièces de rechange.

ÉQUIPEMENT	***PRIX DE LOT:_____ $***

3. INSTALLATION ET FRAIS DE DÉPLACEMENT CONNEXES

Le prix doit comprendre tous les coûts, y compris les dépenses de déplacement et de subsistances, liés à l'installation.

INSTALLATION	***PRIX DE LOT:_____ $***

4. INTÉGRATION ET MISE À L'ESSAI DU LOGICIEL

INTÉGRATION DU LOGICIEL	***PRIX DE LOT:_____ $***
FRAIS DE MISE À L'ESSAI	***PRIX DE LOT:_____ $***

5. FORMATION SUR PLACE ET DOCUMENTATION

COÛT DE LA FORMATION SUR PLACE	***PRIX DE LOT:_____ $***

DESSINS CONFORMES À L'EXÉCUTION DES TRAVAUX	***PRIX DE LOT: _____ $***

MANUELS	***PRIX DE LOT: _____ $***

6. CONTRAT DE SERVICE POUR LE SUPPORT ET LA MAINTENANCE

CONTRAT DE SERVICE	**Prix – 1 année**
Conformément à l'annexe A	$

SOLUTION PROPOSÉE DE L'ENTREPRENEUR pour 340 Laurier (Ottawa)	***PRIX TOTAL DE LA SOUMISSION : _____$*** ***Somme des articles 1 à 6 ci-haut***

PRIX TOTAL DE LA SOUMISSION POUR EVALUATION :

SITE 1

SOLUTION PROPOSÉE DE L'ENTREPRENEUR pour 269 Laurier (Ottawa)	***PRIX TOTAL DE LA SOUMISSION : _____$***

PLUS

SITE 2

SOLUTION PROPOSÉE DE L'ENTREPRENEUR pour 340 Laurier (Ottawa)	***PRIX TOTAL DE LA SOUMISSION : _____$***

PRIX TOTAL DE LA SOUMISSION POUR ÉVALUATION (Site 1 + Site 2)	***PRIX TOTAL DE LA SOUMISSION : _____$***

ANNEXE C PRIX ET BASE DE PAIEMENT (suite)

PARTIE 2 OPTION – EXPANSIONS FUTURE
Les prix seront utilisés pour les Autorisation de tâches

1. POURCENTAGE D'ESCOMPTE DU PDSF POUR ÉQUIPEMENT

Le soumissionnaire doit fournir une liste de fabricants (OEM) représentés et fournir un (1) pourcentage ferme d'escompte sur liste de prix de détail suggéré par le fabricant (PDSF) pour chaque fabricant sur la liste fourni. Le pourcentage d'escompte sera basé sur prix $US seulement si le prix $CDN n'est pas disponible.

Fabricant (OEM)	Pourcentage d'escompte ferme sur PDSF	Pourcentage d'escompte basé sur $US ou $CDN
	%	
	%	
	%	
	%	
	%	
	%	

2. INSTALLATION (TAUX HORAIRES FERMES)

Le soumissionnaire doit soumettre un taux horaire ferme pour l'installation pendant les heures de travail normales et en dehors de celles-ci pour chaque catégorie de main-d'œuvre requise.

Les heures régulières sont du lundi au vendredi, 7h00am à 17h00pm à l'exception des jours fériés.

Catégories de main-d'œuvre	Taux horaire pendant les heures régulières	Taux horaire en dehors des heures régulières
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$

3. INTÉGRATION DU LOGICIEL (TAUX HORAIRES FERMES)

Le soumissionnaire doit soumettre un taux horaire ferme pour l'intégration du logiciel pendant les heures de travail normales et en dehors de celles-ci pour chaque catégorie de main-d'œuvre requise.

Catégories de main-d'œuvre	Taux horaire pendant les heures régulières	Taux horaire en dehors des heures régulières
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$

4. MISE À L'ESSAI DE L'ÉQUIPEMENT (TAUX HORAIRES FERMES)

Le soumissionnaire doit soumettre un taux horaire ferme pour la mise à l'essai de l'équipement pendant les heures de travail normales et en dehors de celles-ci pour chaque catégorie de main-d'œuvre requise.

Catégories de main-d'œuvre	Taux horaire pendant les heures régulières	Taux horaire en dehors des heures régulières
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$

ANNEXE D DE PARTIE 5 – ATTESTATIONS

PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI - ATTESTATION

Je, soumissionnaire, en présentant les renseignements suivants à l'autorité contractante, atteste que les renseignements fournis sont exacts à la date indiquée ci-dessous. Les attestations fournies au Canada peuvent faire l'objet d'une vérification à tout moment. Je comprends que le Canada déclarera une soumission non recevable, ou un entrepreneur en situation de manquement, si une attestation est jugée fausse, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat. Le Canada aura le droit de demander des renseignements supplémentaires pour vérifier les attestations d'un soumissionnaire. À défaut de répondre à cette demande, la soumission sera déclarée non recevable, ou sera considéré comme un manquement au contrat.

Pour obtenir de plus amples renseignements sur le Programme de contrats fédéraux pour l'équité en matière d'emploi, visitez le site Web de Ressources humaines et Développement des compétences Canada - Travail.

Date : _____(AAAA/MM/JJ) [si aucune date n'est indiquée, la date de clôture de la demande de soumissions sera utilisée]

Compléter à la fois A et B.

A. Cochez seulement une des déclarations suivantes :

( ) A1. Le soumissionnaire atteste qu'il n'a aucun effectif au Canada.
( ) A2. Le soumissionnaire atteste qu'il est un employeur du secteur public.
( ) A3. Le soumissionnaire atteste qu'il est un employeur sous réglementation fédérale, en vertu de la *Loi sur l'équité en matière d'emploi*.
( ) A4. Le soumissionnaire atteste qu'il a un effectif combiné de moins de 100 employés au Canada (l'effectif combiné comprend les employés permanents à temps plein, les employés permanents à temps partiel et les employés temporaires [les employés temporaires comprennent seulement ceux qui ont travaillé pendant 12 semaines ou plus au cours d'une année civile et qui ne sont pas des étudiants à temps plein]).

A5. Le soumissionnaire a un effectif combiné de 100 employés ou plus au Canada; et

( ) A5.1. Le soumissionnaire atteste qu'il a conclu un Accord pour la mise en œuvre de l'équité en matière d'emploi valide et en vigueur avec HRDCC - Travail.

OU

( ) A5.2. Le soumissionnaire a présenté l'Accord pour la mise en oeuvre de l'équité en matière d'emploi (LAB1168) à RHDCC - Travail. Comme il s'agit d'une condition à l'attribution d'un contrat, remplissez le formulaire intitulé Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168), signez-le en bonne et due forme et transmettez-le à RHDCC - Travail.

B. Cochez seulement une des déclarations suivantes :

( ) B1. Le soumissionnaire n'est pas une coentreprise.

OU

( ) B2. Le soumissionnaire est une coentreprise et chaque membre de la coentreprise doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi - Attestation. (Consultez la section sur les coentreprises des instructions uniformisées.)

ANNEXE E FORMULAIRE D'AUTORISATION DE TÂCHES PWGSC-TPSGC 572

Voir: http://publiservice-app.pwgsc.gc.ca/forms/pdf/572.pdf

ANNEXE F LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

(voir ci-joint)

ANNEX G ENTENTE DE NON-DIVULGATION – DEMANDE DE SOUMISSIONS ET CONTRAT

(voir ci-joint)

ANNEX H FORMULAIRE DE DEMANDE D'AJUSTEMENT DU TAUX DE CHANGE (PWGSC-TPSGC 450)

(voir ci-joint)

Annexe A

Énoncé des exigences

Sécurité publique Canada – Public Safety Canada (SP/PS)

Sécurité publique/Public Safety –
Système de sécurité intégrée d'entreprise (SSIE de SPPS)

TABLE DES MATIÈRES

TITRE
Système de sécurité intégrée d'entreprise de Sécurité publique/Public Safety (SSIE de SPPS)

OBJECTIF
L'administration centrale de Sécurité publique/Public Safety Canada (SPPS) dans la région de la capitale nationale doit actuellement mettre à niveau son ancien système de contrôle d'accès et des intrusions. Les systèmes actuels sont basés sur 1) Summit Enterprise eNT et 2) ICT Protégé. Il s'agit de passer à un système de sécurité intégrée d'entreprise centralisé et moderne permettant de protéger, de défendre et de répondre aux événements et situations réels et potentiels en matière de sécurité et de sûreté de la vie qui affectent les personnes, les biens et les informations.

SP/PS utilise actuellement le système Summit eNT sur plusieurs étages dans la région de la capitale nationale, au 269, avenue Laurier. Un deuxième bâtiment situé au 340, avenue Laurier est actuellement équipé d'un système indépendant ICT Protégé. Les deux bâtiments utilisent des cartes de proximité commune au même format.

L'objectif de ce contrat est de faire en sorte que les deux bâtiments, avec la possibilité d'autres à l'avenir, fonctionnent dans le cadre d'un seul système intégré centralisé.

Compte tenu de la situation du COVID-19, les restrictions imposées par le gouvernement aux exigences de rassemblements publics et exigences en matière de distance physique, limitent la capacité d'effectuer des visites traditionnelles des lieux. En raison de ses besoins immédiats, Sécurité publique Canada a décidé de distribuer des renseignements détaillés sur ses systèmes actuels aux soumissionnaires intéressés à la suite de la signature d'une entente de non-divulgation. Une téléconférence aura lieu, en remplacement des visites traditionnel, où toutes les questions seront répondu.

SP/PS opère dans de nombreux bureaux régionaux au Canada et la vision à long terme est d'intégrer ces bureaux à la nouvelle plateforme du système. Par conséquent, le système proposé doit pouvoir être étendu en vue de l'intégration future des bureaux régionaux et être contrôlé et géré depuis le 269, avenue Laurier Ouest, Ottawa (Ontario).

SP/PS a besoin d'un contrat d'entretien et de services avec le soumissionnaire retenu à la fin de la mise à niveau (section S).

INTRODUCTION

L'objectif de ce document est de décrire l'énoncé des exigences pour le SSIE de SPPS. Ce document représente une consolidation des exigences techniques et fonctionnelles pour le SSIE de SPPS. Les exigences indiquent l'infrastructure, les caractéristiques et les fonctionnalités du SSIE de SPPS nécessaires pour soutenir le ministère de la Sécurité publique/Public Safety Canada et toutes ses installations au Canada.

La sécurité physique est le moyen par lequel SP/PS met en œuvre des mesures pour protéger les employés, les biens et les renseignements. Les fondements de l'élaboration de cet énoncé des exigences sont les lignes directrices de la GRC relatives à la protection, à la détection et à l'intervention. Bien que le SPPS ait établi une série de normes pour la définition, la conception et la mise en œuvre de stratégies de sécurité physique, ces directives fournissent une méthodologie bien documentée pour des solutions améliorées en matière d'architecture, de technologie et de personnel. Citation tirée du document G1-025 :

> **Des mesures de protection** sont assurées au moyen d'obstacles matériels, et psychologiques visant à exercer un effet dissuasif ou à retarder l'accès non autorisé. Les barrières de protection doivent : dissuader un attaquant, délimiter le périmètre d'une zone restreinte, retarder ou empêcher l'accès, protéger une personne ou un bien contre une menace, contenir une personne ou un bien dans une pièce ou une zone et empêcher la fuite.
>
> Des mesures de **détection** passent par l'utilisation des dispositifs, des méthodes et des procédures qui s'imposent pour que les ministères soient prévenus des tentatives ou des cas réels d'intrusion. La détection comporte quatre étapes distinctes : remarquer l'événement, transmettre l'information concernant l'événement à un centre d'analyse, analyser l'information reçue, évaluer l'information et, si l'événement est jugé non autorisé, déclencher l'intervention.
>
> Dans le contexte de la sécurité matérielle, l'**intervention** consiste à mettre en œuvre des mesures visant à faire en sorte que les incidents ayant trait à la sécurité soient déclarés aux responsables de la sécurité et à ce que des mesures correctrices à court et à long terme soient adoptées en temps opportun. Les stratégies efficaces de planification des interventions doivent être basées sur : les adversaires et leurs qualités, la capacité des intervenants de se rendre au bien ou à la cible et l'habileté des intervenants.

Les aspects techniques de ces éléments clés pour une stratégie de sécurité physique efficace sont décrits dans le contenu de cet énoncé des exigences.

RENSEIGNEMENTS GÉNÉRAUX

Sécurité publique/Public Safety Canada (SP/PS) est l'organisme responsable canadien ayant pour mandat de protéger les Canadiens contre toute une série de risques tels que les catastrophes naturelles, la criminalité et le terrorisme. Sécurité publique Canada travaille avec d'autres ministères fédéraux, d'autres ordres de gouvernement, des premiers intervenants, des groupes communautaires, le secteur privé et d'autres pays pour atteindre ses objectifs. Le Ministère joue un rôle clé dans l'élaboration des politiques, la mise en œuvre des programmes et la cohésion et l'intégration des politiques et des programmes au sein du portefeuille de la sécurité publique, qui comprend la sécurité nationale, la gestion des urgences, l'application de la loi, la gestion des frontières, les services correctionnels et la prévention de la criminalité.

SP/PS a amorcé un projet de mise à niveau, de renouvellement et d'amélioration de ses systèmes vieillissants de contrôle d'accès et d'alarme contre les intrusions qui ont été déployés dans la région de la capitale nationale (RCN). Le présent document a pour objet de définir les exigences techniques et fonctionnelles du SSIE de SPPS. Cette fonctionnalité est nécessaire pour soutenir les objectifs commerciaux des intervenants afin de remplir leurs mandats respectifs. Ce qui suit illustre les fonctionnalités et les capacités du SSIE de SPPS selon les exigences des intervenants.

- Contrôle d'accès électronique
- Gestion et intégration du système d'alarme contre les intrusions
- Infrastructure et sécurité des réseaux
- Entretien, appels de service et intervention
- Opérations de sécurité

CONCEPT DES OPÉRATIONS

Le SSIE de SPPS comprend des logiciels, du matériel et des équipements de sécurité conçus, achetés et installés pour assurer la sûreté, la sécurité et la protection des personnes, des biens et des actifs. Le SSIE de SPPS doit fournir les outils et les applications nécessaires à ses utilisateurs pour gérer les personnes, les biens et surveiller les activités sur le site. Le système est basé sur une infrastructure centralisée à l'administration centrale qui est flexible et configurable pour permettre la bonne gestion des différents processus et procédures afin d'atteindre les objectifs de sécurité de SP/PS. Tout le matériel et les logiciels achetés doivent resté la propriété de SP/PS et, par conséquent, le personnel qualifié de SP/PS du service de sécurité doit avoir un accès libre à tous les aspects et composants du système proposé pendant et après l'installation.

SECTION A – APPLICATIONS DU SSIE DE SPPS

Le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit inclure les applications intégrées de sécurité physique suivantes pour les entreprises :

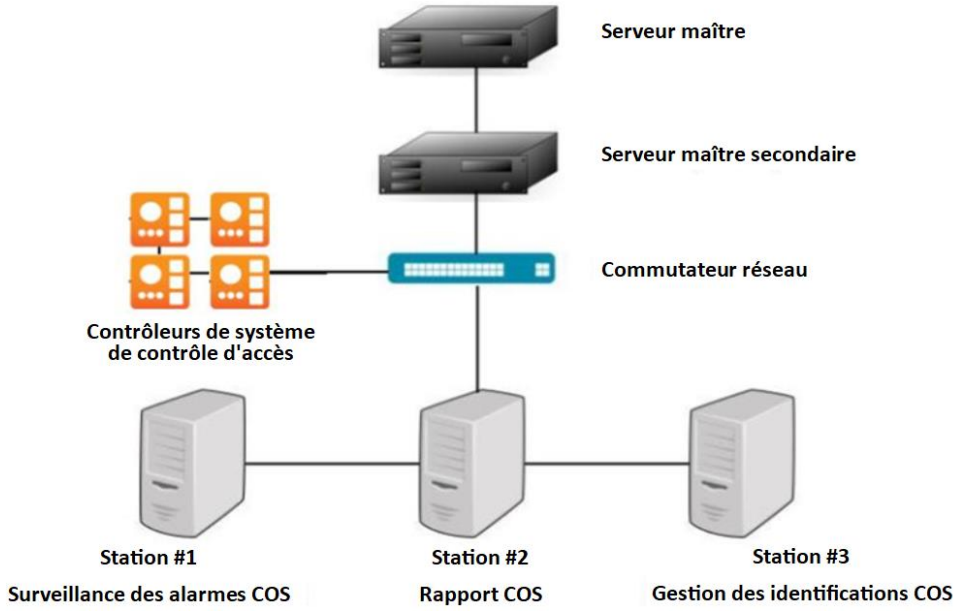
a. Contrôle d'accès électronique
b. Gestion de l'identification du personnel
c. Détection, surveillance, contrôle et signalement des intrusions
d. Contrôle et gestion des entrées et sorties
e. Capacité d'intégration de la vidéosurveillance et de la gestion numériques
f. Gestion des visiteurs
g. Contrôle des ascenseurs
h. Intégration du système de contrainte
i. Rapports de gestion et audit

SECTION B – ARCHITECTURE DU SYSTÈME DE SÉCURITÉ INTÉGRÉE D'ENTREPRISE DE SÉCURITÉ PUBLIQUE/PUBLIC SAFETY (SSIE DE SPPS)

1. Le SSIE de SPPS doit être configuré de telle sorte qu'un serveur maître primaire doit être situé à l'administration centrale au 269, avenue Laurier à Ottawa (Ontario) Canada, sur lequel le logiciel d'application de sécurité et les données et bases de données associées doivent résidé. Le serveur maître primaire doit être accompagné d'un serveur maître secondaire (situé au 340, avenue Laurier Ouest) qui doit être installé dans une configuration entièrement redondante afin d'assurer la fiabilité opérationnelle et l'intégrité des données. Les enregistreurs de télévision en circuit fermé existants, tant à l'administration centrale que sur les deux sites distants, ne font pas partie de ce projet, mais le nouveau système de contrôle d'accès proposé doit avoir les capacité d'intégré à un système vidéo pour afficher la vidéo sur le déclenchement de l'alarme pour les besoins futurs.

Figure 1—Architecture du système central au siège social

Centre des opérations de sécurité

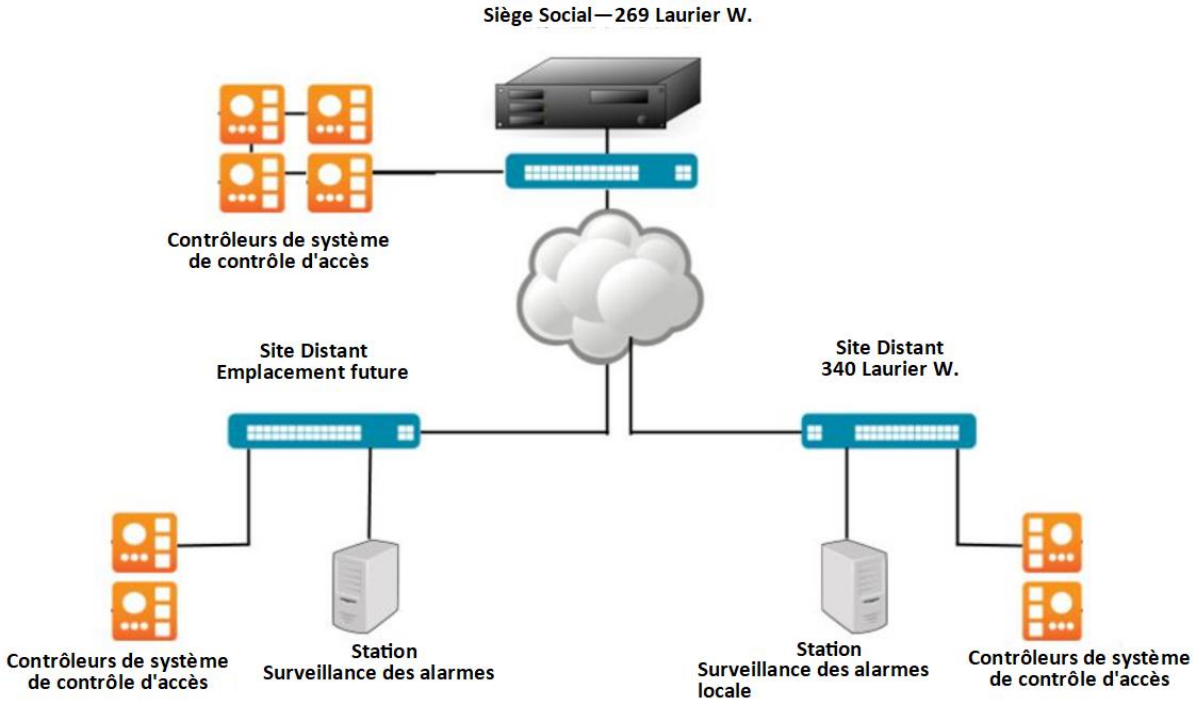


Il incombera au fournisseur de fournir tous les logiciels d'application de sécurité, les licences, le matériel, le câblage réseau des contrôleurs et tout autre périphérique nécessaire pour soutenir l'installation. Les serveurs de réseau, les postes de travail et les commutateurs ne doivent pas être fournis par le fournisseur; ils doivent être achetés à l'interne, mais le fournisseur doit être responsable de communiquer à SP/PS les exigences en matière d'applications et de matériel :

- Serveur(s)
- Postes de travail

Figure 2—Architecture du système réseau au siège social

Emplacement à l'extérieur du siège social



SECTION C – SYSTÈME DE BASE DU SSIE DE SPPS

1. Le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit être basé sur une architecture client-serveur et résidera sur l'infrastructure réseau de SP. Le SSIE de SPPS doit permettre la distribution de fonctions comme la vidéosurveillance, le contrôle d'accès, la surveillance et le contrôle des alarmes, la gestion des accréditations et le traitement des photos d'identité sur le réseau de sorte que ces fonctions soient disponibles à partir de n'importe quel serveur du SSIE de SPPS ou poste de travail du SSIE de SPPS sur le réseau. Le SSIE de SPPS doit s'intégré dans un environnement opérationnel unique et doit utiliser une base de données relationnelle intégrée pour toutes les fonctionnalités.

2. Le SSIE de SPPS doit être fourni dans une architecture entièrement redondante pour chacun des serveurs primaires et secondaires. Le SSIE de SPPS doit prendre en charge les solutions et l'architecture de matériel, de logiciels, de stockage et de produits à haute disponibilité et tolérant les défaillances, et offrira une base de données et une capacité opérationnelle de secours en état d'alerte qui est entièrement redondante. La configuration redondante du SSIE de SPPS doit permettre un fonctionnement normal en cas de défaillance du serveur. Le passage du serveur primaire au serveur de secours (ou secondaire) doit alors être automatique et n'entravera ni ne dégradera le fonctionnement du SSIE de SPPS.

3. Le SSIE de SPPS doit être configuré de telle sorte que les serveurs et postes de travail suivants constituent le cœur du système :
    i. serveur maître 1 (primaire) du SSIE de SPPS (administration centrale);
    ii. serveur maître 2 (secondaire) du SSIE de SPPS (340, avenue Laurier Ouest);
    iii. poste de travail pour opérateur/administrateur du CSP du SSIE de SPPS (administration centrale);
    iv. poste de travail de surveillance des alarmes du CSO du SSIE de SPPS (administration centrale);
    v. poste de travail de gestion des identifications du SSIE de SPPS (administration centrale);
    vi. poste de travail de surveillance des alarmes du SSIE de SPPS (site distant).

4. Le serveur maître primaire du SSIE de SPPS doit résider à l'administration centrale à Ottawa (Ontario) Canada et doit contenir toutes les données et fonctionnalités opérationnelles et administratives pour l'ensemble du SSIE de SPPS. Le serveur maître secondaire doit être situé dans un autre bâtiment (340, avenue Laurier Ouest). Le SSIE de SPPS doit prendre en charge la future configuration de reprise après sinistre (RS) dans un lieu hors site dans l'éventualité où les serveurs principal et secondaire ne seraient pas accessibles. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

5. Le poste de travail pour opérateur/administrateur du SSIE de SPPS doit permettre la configuration, la gestion et la communication de tous les paramètres de programmation du

système, des fonctions d'identification, de la programmation des alarmes et des événements et du fonctionnement du matériel. Il peut également servir de poste de travail pour la formation des nouveaux gardiens du Centre de sécurité opérationnel. Les droits des utilisateurs doivent régir les privilèges d'accès (lecture/écriture) aux applications, modules, données et dossiers du SSIE de SPPS.

6. Le poste de travail de surveillance des alarmes du SSIE de SPPS doit permettre de surveiller et de signaler les alarmes et les événements du système de contrôle d'accès. Les droits des utilisateurs doivent régir les privilèges d'accès (lecture/écriture) aux applications, modules, données et dossiers du SSIE de SPPS.

7. Le poste de travail de gestion des identifications du SSIE de SPPS (site distant) doit permettre l'inscription des titulaires de justificatifs d'identité, la saisie des photographies, la signature et des données du titulaire de justificatifs d'identité et la génération de justificatifs d'identité physiques (p. ex., des cartes d'identification avec photo). Les droits des utilisateurs doivent régir les privilèges d'accès (lecture/écriture) aux applications, modules, données et dossiers du SSIE de SPPS. *La gestion de l'identification, de même que l'impression et la conception des cartes doivent être compatibles avec les équipements existants :

8. Le poste de travail de surveillance des alarmes du SSIE de SPPS (site distant) doit fournir une installation hors site pour la surveillance locale et la notification des alarmes et des événements du système de contrôle d'accès. Les droits des utilisateurs doivent régir les privilèges d'accès (lecture/écriture) aux applications, modules, données et dossiers du SSIE de SPPS.

9. Le système doit être composé des principaux éléments suivants :
    i. serveur maître (primaire) du SSIE de SPPS, serveur maître (secondaire) du SSIE de SPPS, poste de travail de l'administrateur du SSIE de SPPS, postes de travail de surveillance des alarmes du SSIE de SPPS et poste de travail de gestion des identifications du SSIE de SPPS;
    ii. réseau sécurisé;
    iii. dispositifs et composants de réseau;
    iv. panneaux de commande;
    v. dispositifs et composants de sécurité (p. ex., lecteurs de justificatifs, dispositifs de verrouillage, capteurs d'alarme).

10. Chacune de ces composantes majeures doit s'intégrée pour fonctionner comme une solution de système clé en main complète et pleinement fonctionnelle.

11. Il est obligatoire que le SSIE de SPPS proposé englobe et tire parti des dispositifs de contrôle d'accès déjà installés à chaque porte. Cela inclut notamment les dispositifs suivants :

    i. lecteurs de cartes - (à remplacer par un nouveau);

ii. dispositifs de demande de sortie – Kantech T-Rex;
iii. contacts de porte – divers;
iv. installation de gâches – 12 V c.c./24 V c.c. – divers;
v. leviers électrifiés – 24 V – divers;
vi. sirènes/piézoélectrique – 12-24 V c.c. – divers.

12. Tout poste de travail du SSIE de SPPS sur le réseau doit être en mesure d'effectuer la saisie de données, le traitement et la gestion des alarmes et les fonctions de gestion du système.

13. L'architecture du SSIE de SPPS doit être flexible et évolutive, permettant l'expansion de la capacité et des fonctionnalités; elle sera mise en œuvre progressivement selon les besoins au moyen de licences et de mises à jour de logiciels tout en maintenant les opérations du réseau.

14. Le SSIE de SPPS doit permettre, sans toutefois l'exiger, la séparation des rôles du serveur de base de données, du serveur de fichiers, du serveur d'application et du serveur Web afin de soutenir l'architecture du serveur à plusieurs niveaux.

15. Le SSIE de SPPS doit être en mesure de prendre en charge la réplication de bases de données et de fichiers, comme les services de réplication de serveurs Microsoft SQL et la Réplication du système des fichiers distribués (DFS-R) de Microsoft, afin de fournir une réplication de bases de données distribuées sur les serveurs d'applications du SSIE de SPPS. Cela permettra l'extension du système et offrira des niveaux de redondance pour les serveurs. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

16. Le SSIE de SPPS doit être conçu selon une architecture sur IP et doit être conforme aux protocoles de communication TCP/IP standard entre ses composants, y compris les capacités de routage et de traversée de pare-feu.

17. Il est nécessaire que le SSIE de SPPS soutienne une stratégie de zonage imbriquée ou à plusieurs niveaux, de sorte que les zones publiques, d'accueil, d'exploitation, de sécurité et de haute sécurité puissent être gérées de manière indépendante et interactive. Il est nécessaire que ces zones soient définies dans le SSIE de SPPS et comprennent divers dispositifs d'accès (p. ex., des lecteurs, des claviers) ou d'intrusion (p. ex., des détecteurs de mouvement, des contacts de porte, des claviers de contrôle d'alarme locale). Une fois qu'une zone est définie, le SSIE de SPPS doit permettre de programmer la posture et le fonctionnement de chaque zone indépendamment. Voici quelques exemples de ces postures : masquer toute la zone, démasquer toute la zone, ou définir des règles anti-retour entre les zones. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

18. Pendant la durée du contrat, le fournisseur doit veiller à ce que tous les panneaux de commande et les modules associés soient rétrocompatibles. Le fournisseur doit veiller également à ce que tous les panneaux de commande et le matériel associé fournis pendant la durée du contrat soient supportés par les versions, les mises à jour, les mises à niveau et

les versions de maintenance les plus récentes des logiciels et des microprogrammes. Le fournisseur doit s'assurer également que toutes les alimentations électriques, les batteries et les convertisseurs de puissance sont adéquats pour soutenir les installations.

SECTION D – EXIGENCES EN MATIÈRE DE PLATEFORME ET D'INFRASTRUCTURE

Comme le SSIE de SPPS s'appuie sur notre infrastructure de réseau interne pour transporter, traiter et stocker ses accès, ses vidéos d'alarme et d'autres informations et données, il est essentiel que le SSIE de SPPS réponde aux normes, politiques, programmes et équipements de TI/GI de SPPS. La section suivante décrit les exigences associées aux normes de la plateforme informatique du ministère, aux bases de données, à l'architecture et aux stratégies de réseau, aux politiques de sécurité informatique, aux environnements particuliers des systèmes d'exploitation et des applications et à d'autres éléments techniques qui doivent être satisfaits par le nouveau SSIE de SPPS.

Plateforme et environnement opérationnel

1. Le SSIE de SPPS doit fonctionner sur une plateforme matérielle de serveur qui est adéquate pour les besoins du système proposé et qui offre toutes les capacités de traitement, de mémoire, de stockage et de mise en réseau pour faire fonctionner le système de manière fiable. Les serveurs doivent être hébergés par d'autres dans un environnement de centre d'opérations de sécurité opérationnelle.

2. Le SSIE de SPPS doit fonctionner sur une plateforme matérielle de postes de travail qui répondra aux exigences du système proposé et qui aura suffisamment de capacités de traitement, de mémoire, de stockage et de mise en réseau pour fonctionner de manière fiable. Les postes de travail doivent être hébergés par d'autres dans des zones d'opération sécurisées.

3. Le matériel du SSIE de SPPS doit communiquer sur la topologie actuellement existante et permettra une communication sécurisée. Le fournisseur doit s'assurer que le matériel fourni communiquant sur le réseau a la capacité de cryptage sécuritaire grâce à des configurations appropriées.

4. L'application du SSIE de SPPS ne doit pas nécessiter de dispositifs physiques distincts (p. ex., des clés matérielles) pour l'octroi de licences ou le fonctionnement.

5. Tous les appareils du SSIE de SPPS dotés d'une horloge système doivent se synchroniser sur l'heure du réseau du serveur primaire en utilisant le service de temps Windows sur le Protocole de temps du réseau (PTR).

6. Le SSIE de SPPS doit utiliser au minimum la base de données Microsoft SQL Server 2012 et doit fonctionner en mode normal.

7. Les clients du SSIE de SPPS doivent utiliser un environnement de système d'exploitation Windows 10 ou plus récent.

8. Le SSIE de SPPS doit fonctionner dans l'environnement Windows Server 2012 ou dans un système d'exploitation plus récent.

9. Le SSIE de SPPS doit prendr en charge les installations et les mises à jour de logiciels et de micrologiciels sans surveillance. En particulier, tous les microprogrammes doivent être téléchargeables sans avoir à se rendre sur place pour effectuer une mise à niveau.

Interface utilisateur

10. Le SSIE de SPPS doit utiliser une interface utilisateur graphique (IUG) intuitive, conforme aux normes de l'industrie et compatible avec Windows pour toutes les opérations d'administration, d'utilisation et de configuration. L'interface utilisateur doit fournir un environnement intuitif au personnel opérationnel pour qu'il puisse gérer les fonctions, notamment la surveillance et le contrôle des dispositifs du système comme les capteurs d'alarme et les serrures de porte par une méthode simple de pointer-cliquer. Il est également nécessaire que l'interface utilisateur offre l'aspect et la convivialité familiers des environnements de bureau actuels basés sur Windows en permettant à l'opérateur de visualiser le système (et ses opérations) dans un format graphique. Il est nécessaire de mettre en place une barre d'outils composée d'un ensemble d'icônes liées à l'action pour permettre un contrôle aisé du système. Il est nécessaire que le système offre également des fonctions complètes de recherche et de tri.

11. Les utilisateurs ne doivent pas avoir besoin de disposer de droits d'administrateur Windows pour lancer, configurer ou utiliser l'application du SSIE de SPPS. Dans le SSIE de SPPS, les utilisateurs doiven avoir les droits d'administrateur Windows pour pouvoir installer ou mettre à jour le logiciel.

12. Il est souhaitable que le SSIE de SPPS prenne en charge des modules utilisant une interface Web et s'intègre à Microsoft Internet Explorer, ainsi qu'à Google Chrome pour que le navigateur prenne en charge des fonctions précises et largement utilisées. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

Sécurité informatique

13. Le SSIE de SPPS doit être déployé (et fonctionnera) dans un environnement de sécurité des TI. Le système proposé exige au minimum ce qui suit :

    i. chaque utilisateur doit être identifié de manière unique. Aucun accès en réseau aux ressources et aux données du SSIE de SPPS ne doit être autorisé sans que l'utilisateur ne soit identifié de manière unique;

ii. les mots de passe doivent comporter au minimum 8 caractères et doivent respecter les caractéristiques suivantes : contenir au moins trois des quatre éléments suivants : chiffre, caractère spécial, majuscules, minuscules. Les 8 mots de passe précédents ne doivent pas être réutilisés;
iii. l'opérateur doit être obligé de se connecter à un poste de travail du SSIE de SPPS après 15 minutes d'inactivité (du client) et 15 minutes d'inactivité (du serveur). Le poste de travail de surveillance de l'alarme ne doit jamais se verrouiller et doit toujours être disponible pour répondre à une alarme;
iv. le SSIE de SPPS doit permettre qu'un enregistrement de tous les événements et actions de sécurité importants concernant des utilisateurs et des administrateurs doivent être conservé dans des journaux d'audit protégés.

14. Le SSIE de SPPS doit utiliser le SMTP crypté pour toutes les communications de messagerie sur le réseau.

15. Toutes les bases de données du SSIE de SPPS doivent supporter des mécanismes de sécurité des données limitant l'accès non autorisé et empêchant l'altération des données stockées. Ces mécanismes de sécurité doivent garantir l'intégrité, la disponibilité et la confidentialité des données du SSIE de SPPS.

16. En fonction des privilèges de l'utilisateur et de la configuration du poste de travail ou du serveur, l'utilisateur pourra effectuer toute saisie de données, gestion d'alarme, configuration et gestion du système à partir de n'importe quel poste de travail du SSIE de SPPS sur le réseau.

17. Le SSIE de SPPS doit fournir une fonction d'autorisation d'utilisateur basée sur les rôles. Les administrateurs du système doivent avoir la possibilité de définir des utilisateurs ou des groupes d'utilisateurs auxquels des autorisations sélectives sont accordées (p. ex., des applications particulières, des enregistrements – ajout, modification, suppression). Les utilisateurs peuvent être affectés à un ou plusieurs groupes. Les groupes d'utilisateurs doivent être appelés groupes composés d'utilisateurs ou groupes d'utilisateurs.

18. Il est interdit au fournisseur ou à tout entrepreneur qui travaille sur le système, qui utilise un appareil appartenant au Gouvernement du Canada/GCnet ou qui se branche sur du matériel (p. ex., un interrupteur) d'utiliser des clés USB, des ordinateurs ou des ordinateurs portatifs externes. Si des clés USB sont requises, elles doivent être communiquées à SP/PS, et si elles sont acceptées, elles doivent être scannées par la sécurité des TI AVANT d'être branchées à un ou plusieurs appareils faisant partie de l'infrastructure réseau du Gouvernement du Canada.

Intégration avec des applications tierces

19. Le SSIE de SPPS doit être compatible avec, au minimum, Microsoft Office 2013, y compris Outlook, Excel et Word.

20. Le SSIE de SPPS doit être compatible avec Adobe Acrobat Reader (V11 ou supérieur) pour la visualisation des documents.

21. Les systèmes, modules, applications et composants du SSIE de SPPS doivent disposer d'une feuille de route documentée pour prendre en charge les futures versions des produits, du système d'exploitation et des bases de données Microsoft au cours des dix prochaines années. Il doit, au minimum, traiter de la sécurité et des applications de Windows Server et du système d'exploitation de bureau, de Microsoft SQL Server, de Microsoft Internet Explorer et des applications du SSIE de SPPS. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

Soutien aux fuseaux horaires

22. Le SSIE de SPPS doit prendre en charge chaque fuseau horaire standard dans le monde et maintiendra l'intégrité de la date et de l'heure de toutes les configurations du système, des transactions et des rapports provenant de divers endroits futurs.

23. Le SSIE de SPPS doit enregistrer, suivra et maintiendra l'heure locale au serveur, et l'heure locale de chaque panneau de commande (serveur PTR). Le SSIE de SPPS doit gérer chacune de ces heures individuelles de manière à ce que les alarmes, les événements et les transactions doivent être horodatés à leur origine et que ces horodatages originaux soient conservés, quel que soit l'endroit où ils sont déclarés ou gérés. Cette intégrité temporelle doit maintenue à tout moment.

24. Il est souhaitable que le SSIE de SPPS soutienne la gestion du système afin de prendre en charge les heures d'été spécifiques à chaque localité ou site, le cas échéant. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

Connectivité

25. Comme le SSIE de SPPS doit communiquer sur un certain nombre de types de réseaux physiques différents, le système doit être tolérant à la perte de paquets de réseau, pourra se remettre des pannes de réseau et disposera d'un moyen d'indiquer aux utilisateurs que les conditions du réseau ont une incidence sur le rendement du système. En cas de panne de réseau ou d'électricité, chaque contrôleur en réseau doit se connecter automatiquement et ne doit pas nécessiter de processus de démarrage manuel de la part d'un opérateur ou d'un utilisateur.

26. Tous les sous-systèmes du SSIE de SPPS doivent être sensibles à la qualité de service (QoS) et prendront en charge la planification des files d'attente de QoS du réseau pour

le trafic multimédia et hautement prioritaire. Les événements et les alarmes générés au sein et par le SSIE de SPPS doivent être la plus haute priorité.

27. Tous les systèmes et applications du SSIE de SPPS doivent utilisé des adresses réservées attribuées par Protocole de configuration d'hôte dynamique (DHCP) pour les serveurs et les nœuds, et non des adresses IP fournies statiquement (sauf si l'équipement réseau existant le permet). Les adresses IP statiques doivent être utilisées pour certains dispositifs de sécurité comme les panneaux de commande. Les serveurs doivent avoir la capacité de gérer les protocoles DNS.

28. Le système sélectionné doit avoir la capacité et inclure toutes les licences de logiciels permettant d'exécuter des applications de Remote Desktop Protocol (RDP). Il est souhaitable que le système fonctionne dans un environnement Citrix. Il n'est pas nécessaire de mettre en œuvre Citrix à cette étape, mais cela le sera pour les besoins futurs.

Active Directory

29. Le SSIE de SPPS doit prendre en charge une connexion directe à un serveur Microsoft de l'application Active Directory. L'intégration d'Active Directory doit permettre la synchronisation des informations du serveur Active Directory avec les serveurs du SSIE de SPPS.

30. Lorsqu'il est activé, Active Directory doit gèrer la connexion de l'utilisateur aux applications clientes du SSIE de SPPS à l'aide des informations d'identification Windows de l'utilisateur.

31. Il doit possible de synchroniser les entités du SSIE de SPPS suivantes et leurs informations à partir
    d'Active Directory au SSIE de SPPS :

    i. utilisateurs (nom d'utilisateur, prénom et nom de famille, adresse électronique, etc.);
    ii. groupes d'utilisateurs (nom du groupe d'utilisateurs, description et adresse électronique du groupe);
    iii. titulaires de justificatifs d'identité (nom et prénom, description, courriel, etc.).

32. Il est nécessaire que, lorsqu'il est activé, l'ajout, la suppression ou la suspension du compte Windows d'un utilisateur dans Active Directory entraîne la création, la suppression ou la désactivation du compte d'utilisateur équivalent dans le SSIE de SPPS. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

33. Il est nécessaire que, lorsqu'il est activé, l'ajout, la suppression ou la suspension du compte Windows d'un utilisateur dans Active Directory entraîne la création, la

suppression ou la désactivation du compte du titulaire de justificatifs d'identité équivalent dans le SSIE de SPPS. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

SECTION E – CONFORMITÉ AUX NORMES

1. Le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit être conforme aux normes suivantes : la norme de sécurité UL 294 (Access Control System Units) et UL 1076 (Proprietary Alarm Units) ou la norme CAN/LAC S319-05 (Electronic Access Control Systems) et CAN/LAC 302-M91 (R1999) (Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults). Décrivez comment le SSIE de SPPS proposé soutient cette exigence, le cas échéant.

2. Le SSIE de SPPS doit prendre en charge les communications cryptées approuvées entre les serveurs et d'autres serveurs, entre les serveurs et les postes de travail et entre les serveurs et les panneaux de commande. Les données de l'application et le trafic réseau doivent être cryptés au niveau AES 128 ou mieux. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

3. Le fournisseur doit appliquer un programme de gestion de la qualité dans le développement, la fabrication et le soutien de ses produits matériels et logiciels. Il est souhaitable que le fournisseur possède un programme de gestion de la qualité mis en œuvre (p. ex., certification ISO).

4. Le SSIE de SPPS doit intégrer des politiques de sécurité réseau et de pare-feu comme décrites dans la directive ITSG-22 du Centre de la sécurité des télécommunications Canada (CSTC). Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

SECTION F – INTÉGRATION

1. Le SSIE de SPPS doit être intégré aux systèmes de vidéosurveillance pour l'évolution future. Décrivez les systèmes de vidéosurveillance les mieux adaptés ou susceptibles de s'intégrer (interface de programmation d'applications, kit de développement logiciel) au système proposé.

2. Le SSIE de SPPS a pour mandat d'installer environ 60 portes dans la RCN (les deux sites répertoriés), 40 portes pour le 269, avenue Laurier et 20 portes pour le 340, avenue Laurier. Le fournisseur doit fournir tous les coûts de matériel, de logiciel et de main-d'œuvre pour intégrer les 60 opérateurs de portes automatiques nouvellement installés au moment de l'installation, qui peut avoir lieu en dehors des heures de travail.

3. Il est nécessaire que le SSIE de SPPS puisse agir lors d'un événement de confinement à l'échelle du système (ou d'une zone), par exemple lors d'un incident mettant en cause un tireur actif.

SECTION G – EXTENSIBILITÉ

1. Le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit être conçu et élaboré pour soutenir la croissance future du système, notamment en ajoutant des dispositifs d'accès, système d'alarme, des caméras, des postes de travail et des serveurs sans modifications majeures du matériel ou des logiciels. Le SSIE de SPPS doit pouvoir être intégré progressivement à tous les bureaux régionaux de SP (liste des emplacements dans la SECTION Q) et être géré et contrôlé depuis l'administration centrale de SP à Ottawa (ON).

Le soumissionnaire doit être en mesure d'offrir l'installation et le service à nos bureaux régionaux situés dans les villes énumérées dans la section Q dans le cadre d'une AUTRE phase pour une extension et une utilisation futures de ce contrat.

2. Le SSIE de SPPS doit être un système extensible qui prendra en charge au minimum les dispositifs de sécurité suivants :

i. deux serveurs de système (un primaire, un secondaire);
    a. maître primaire – AC;
    b. maître secondaire – 340, avenue Laurier Ouest;
    c. quatre postes de travail pour le système;

ii. 12 utilisateurs sur 5 postes de travail ou serveurs du SSIE de SPPS, dont 5 sont actifs simultanément et à tout moment;
iii. 200 panneaux de commande;
iv. 1 500 lecteurs de justificatifs d'identité ou claviers;
v. 6000 capteurs d'alarme;
vi. 3500 dispositifs de sortie de relais;
vii. soutien local et technique pour chaque fuseau horaire standard au Canada;
viii. 25 000 titulaires de justificatifs d'identité.

SECTION H – GESTION DES DROITS DES UTILISATEURS

1. Le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit prendre en charge un nombre illimité d'utilisateurs du système, de groupes d'utilisateurs et de mots de passe. Le système doit permettre de limiter les capacités des utilisateurs ou de groupes d'utilisateurs précis à un groupe de fonctions définies. Le SSIE de SPPS doit permettre également à l'administrateur de limiter les utilisateurs ou les groupes pouvant accéder à des enregistrements de justificatifs d'identité et à des panneaux particuliers ainsi qu'à des

enregistrements d'entrée ou de sortie. Le SSIE de SPPS doit fournir un mécanisme permettant de synchroniser les utilisateurs d'Active Directory avec les utilisateurs du SSIE de SPPS, de sorte que l'ajout et la suppression d'utilisateurs ne nécessitent pas de nouvelle saisie manuelle des données.

2. Le SSIE de SPPS doit permettre de définir les droits des utilisateurs pour les modules, les fonctions et les capacités de configuration « Créer », « Lecture », « Mettre à jour » et « Supprimer » :

i. justificatifs de contrôle d'accès;
ii. utilisateurs;
iii. opérateurs;
iv. alarmes;
v. reconnaissance des alarmes;
vi. configurer les horaires de vacances du système;
vii. configurer les groupes de systèmes;
viii. configurer le matériel du SSIE de SPPS;
ix. configurer le matériel du réseau;
x. configurer les serveurs du système;
xi. créer et produire des rapports que l'utilisateur final peut sélectionner.

SECTION I – PANNEAUX DE COMMANDE

1. Le panneau de commande assure le lien entre le serveur du SSIE de SPPS et ses composants matériels comme les lecteurs de justificatifs, les serrures de porte, les capteurs d'alarme et les périphériques de sortie. Chaque panneau de commande doit disposer de toutes les installations de traitement, de mémoire et d'entrée/sortie pour prendre en charge chacun de ses dispositifs respectifs, comme décrit à la section I.5 ci-dessous. Le panneau de commande doit être basé sur la technologie des microprocesseurs et offrira des opérations totalement autonomes. Lors de l'initialisation du système, il doit être possible de télécharger toutes les données d'exploitation et de titulaire de justificatifs d'identité vers le panneau de commande à partir du serveur maître du SSIE de SPPS, ou de n'importe quel poste de travail. La défaillance d'un panneau de commande ne doit pas affecter le fonctionnement des autres panneaux de commande du réseau. Le logiciel et le micrologiciel du panneau de commande doivent être programmés dans un langage de haut niveau pour faciliter la maintenance et l'amélioration des fonctionnalités. Chaque panneau principal, sous-panneau et tout autre matériel doivent être situés dans une salle sécurisée centralisée.

2. Il incombe au fournisseur de s'assurer que tous les câblages nécessaires, l'équipement et les outils spécialisés, ainsi que toutes les alimentations électriques sont adéquats pour supporter chaque installation. En cas de problème, il incomber au fournisseur, à ses frais, d'assurer le bon fonctionnement du système.

3. Tous les codes opérationnels des panneaux de commande sont stockés dans une mémoire morte non volatile, tandis que les paramètres du système et les données de contrôle d'accès sont stockés dans une mémoire RAM sauvegardée par une batterie. Chaque panneau de commande doit prendre en charge des logiciels téléchargeables, en utilisant la mémoire flash intégrée. Les téléchargements instantanés des nouveaux logiciels intégrés doivent être conditionnés et se feront de manière transparente.

4. Chaque panneau de commande doit contienir une horloge intégrée en temps réel alimentée par une batterie pour le contrôle d'accès, le déclenchement d'événements et l'horodatage aux dossiers. L'horloge du panneau de commande doit être synchronisée à partir du serveur du site SSIE de SPPS.

5. Le panneau de commande doit supporter des niveaux de tension d'entrée d'environ 120 V CA, 60 Hz et comprendra des alimentations à découpage et des batteries appropriées pour fournir une alimentation de secours opérationnelle de 8 heures en cas de perte de courant alternatif. Le panneau de commande doit utiliser des batteries de secours communes, conformes aux normes industrielles, qui seront généralement disponibles dans le commerce. Le panneau de commande doit signaler toute perte de puissance ou tout état de batterie faible au serveur. Chaque panneau de commande doit être doté d'une fonction de redémarrage automatique qui permettra un démarrage automatique après la mise sous tension. Le panneau de commande passera automatiquement en mode de sauvegarde sur batterie en cas de perte de courant alternatif. Toute connexion électrique au-delà de ce qui est déjà installé à chaque panneau existant est de la responsabilité du fournisseur, et doit être coordonnée avec le bâtiment de base de chaque emplacement. Le client peut aider à la coordination des installations selon les besoins.

6. Chaque panneau de commande du SSIE de SPPS doit prendre en charge un minimum de 25 000 titulaires de justificatifs d'identité, un minimum de 8 lecteurs de justificatifs d'identité, un minimum de 12 points d'entrée d'alarme et 12 points de sortie de relais.

7. Le SSIE de SPPS doit être en mesure de se connecter à des lecteurs de cartes Wiegand compatibles et de les gérer. Les panneaux de commande et les lecteurs doivent prendre en charge plusieurs codes d'installation.

8. Le panneau de commande doit être en mesure de contrôler l'accès et de signaler les alarmes simultanément.

9. Le panneau de commande doit appuyer les opérations des portes à des horaires variables. Par exemple, le SSIE de SPPS (et le panneau de commande en mode hors ligne) doit prendre en charge le fonctionnement du lecteur uniquement de 8 h à 17 h et le lecteur/clavier de 17 h à 8 h.

10. Le panneau de commande doit communiquer en permanence avec le serveur SSIE de SPPS afin de signaler la réception d'une condition d'alarme, de télécharger des lectures de justificatifs d'identité ou de recevoir des modifications des paramètres de fonctionnement ou des données. Le panneau de commande doit fonctionner de manière autonome, de sorte que toutes les décisions de contrôle d'accès soient prises sur la base de la vérification d'un justificatif d'identité individuel par rapport aux paramètres de contrôle d'accès et aux données stockées au panneau de commande. Cette vérification doit porter sur l'identité, l'heure et le code de l'installation à tout moment, même en mode autonome. Les vérifications dégradées de codes autres que ceux des installations ne sont pas acceptables.

11. Le panneau de commande du SSIE de SPPS doit communiquer via Ethernet 10/100/1000 Mo et doit avoir la capacité de résider sur un réseau local (LAN) ou un réseau étendu (WAN) sans connexion à un port série de l'ordinateur.

12. Le panneau de commande doit prendre en charge la connexion Ethernet 10/100/1000 Mo au serveur SSIE de SPPS. Les dispositifs en aval du panneau de commande peuvent être de type RS-485 ou équivalent si nécessaire.

13. Il est souhaitable que l'initialisation complète et le téléchargement des instructions d'utilisation du panneau de commande et de la base de données des titulaires de justificatifs d'identité (au nombre de 25 000) ne prennent pas plus de 5 minutes lorsqu'ils sont connectés via Ethernet 10/100 Mo. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

14. Le panneau de commande doit contenir des diodes électroluminescentes (DEL), qui affichent à la fois l'état de transmission et de réception du serveur local du SSIE de SPPS. Les DEL doivent indiquer également l'état de l'alimentation électrique fournie directement ou par le système de sauvegarde sur batterie.

15. Toutes les données de fonctionnement du système doivent être stockées dans les serveurs principaux primaire et secondaire du SSIE de SPPS et doivent automatiquement téléchargées dans le panneau de commande une fois sauvegardées dans la base de données du SSIE de SPPS. Toutes les modifications apportées à la base de données (p. ex., l'ajout, la suppression ou la modification de données par le titulaire de justificatifs d'identité) doivent être envoyées de manière cryptée aux panneaux de commande en temps réel lorsque tout élément de données pertinent est modifié.

16. Il doit être possible de définir l'heure locale dans chaque bureau ou installation régional. Cette heure doit être appliquée à chaque panneau de commande et poste de travail du SSIE de SPPS dans l'installation. L'heure de toutes les transactions d'accès et d'utilisation, les alarmes, les événements et les activations de sortie, par exemple, doivent être horodatés à l'heure locale au bureau ou à l'installation. Le serveur doit recevoir ces transactions et conservera l'horodatage des données reçues des dispositifs du bureau ou de l'installation (p. ex., le panneau de commande).

17. Le temps de réponse entre la présentation d'un justificatif d'identité valide et la réussite de l'autorisation d'accès à la porte ou au portail doit être inférieur à une seconde. Toutes les demandes d'accès doivent être traitées localement au sein du panneau de commande.

18. Tous les panneaux et sous-modules de sécurité doivent être logés dans des boîtiers verrouillés et inviolables qui limiteront l'accès ou les dommages accidentels et contiendront et disposeront d'interrupteurs d'inviolabilité opérationnels.

19. Chaque panneau de commande du SSIE de SPPS doit être en mesure de fonctionner de manière autonome sans connexion réseau. En fonctionnement autonome, les panneaux de commande doivent conserver toutes leurs fonctionnalités (à l'exception de l'affichage des alarmes sur un poste de travail du SSIE de SPPS) en utilisant les données de contrôle d'accès stockées localement et doivent conserver toutes les transactions de contrôle d'accès et d'alarme. Les renseignements transactionnels (y compris les données d'alarme) doivent être récupérés par le serveur du SSIE de SPPS lorsque la connexion réseau sera rétablie. Le SSIE de SPPS doit stocker un minimum de 5 000 transactions d'accès et 5 000 alarmes/événements, au minimum, avant d'écraser les événements les plus anciens.

20. Des alarmes spécifiques aux panneaux de commande doivent être définies pour les pertes de courant alternatif, les erreurs de communication et l'altération des boîtiers des panneaux de commande.

21. Il doit être possible d'acheter des contrôleurs, des modules, des alimentations électriques et d'autres équipements faisant partie intégrante des panneaux de commande (sans châssis) auprès du fournisseur.

22. Les garanties des panneaux de commande doivent être maintenues, quelles que soient les méthodes de montage et de configuration existantes ou nouvelles, à condition que les directives d'installation soient respectées.

23. Le SSIE de SPPS doit soutenir l'utilisation de résistances de fin de ligne pour surveiller les conditions de sabotage des lignes. Le SSIE de SPPS doit supporter jusqu'à deux configurations de résistance de fin de ligne sur une seule paire de fils desservant un ou deux appareils. Le SSIE de SPPS doit prendre en charge des modules de résistance pour assurer une telle supervision, par exemple dans des conditions d'ouverture, de fermeture, de coupure et de court-circuit.

24. Il est souhaitable que les exigences de fonctionnement et de stockage du panneau de commande soient :

    i. Température de stockage : 0 °C à 50 °C
    ii. Humidité relative de stockage : 0 à 95 % H. R. (sans condensation)
    iii. Température de fonctionnement : 0 °C à 50 °C

iv. Humidité relative de fonctionnement : 0 à 80 % H. R. (sans condensation)

25. Il est souhaitable que le panneau de commande utilise de l'époxy ignifuge dans ses cartes de circuits imprimés et ses composants classés UL/CSA, le cas échéant.

Il est souhaitable que chaque panneau de commande :

i. soit conforme aux règles de la classe A de la partie 15, sous-partie B, de la FCC des États-Unis;
ii. soit conforme à la directive 73/23/CEE de la CSA 22.2 950;
iii. ait la désignation NRTLC/C de la CSA et réponde aux normes de sécurité canadiennes et américaines;
iv. ait la désignation CE.

SECTION J – CONTRÔLE D'ACCÈS

1. Le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit fournir des capacités de contrôle d'accès distribuées et complètes. Le SSIE de SPPS doit utiliser des serveurs et des postes de travail, des panneaux de commande et des lecteurs de justificatifs électroniques pour définir les paramètres d'accès des utilisateurs et contrôler l'accès aux bâtiments et aux zones.

2. Toutes les fonctions standard de configuration et de stockage du contrôle d'accès doivent être fournies par les serveurs principaux du SSIE de SPPS, ainsi que par les postes de travail du SSIE de SPPS. Ces fonctions doivent comprendre notamment :
    i. saisie des données de configuration du contrôle d'accès;
    ii. saisie des données d'exploitation du contrôle d'accès;
    iii. stockage et affichage des données de contrôle d'accès;
    iv. téléchargement des données relatives au statut de l'utilisateur dans les panneaux de commande;
    v. modification des données de contrôle d'accès;
    vi. archivage des transactions d'accès;
    vii. récupération des dossiers d'accès auprès du ou des panneaux de commande;
    viii. modification/affichage du statut de titulaire de justificatifs d'identité;
    ix. intégration du module de contrôle d'accès aux autres modules du SSIE de SPPS;
    x. génération de rapports de gestion et d'archivage/transaction.
    xi. Intégration de carte/plan d'étage

3. Le SSIE de SPPS doit prendre en charge jusqu'à 25 000 titulaires de justificatifs d'identité.

4. Le SSIE de SPPS doit prendre en charge la gestion de l'accès à un certain nombre de types de portails différents, y compris, mais sans s'y limiter, les portes d'accès simples et doubles, les portes actionnées/assistées pour handicapés*, les sas, les tourniquets, les portes basculantes, les portails de véhicules et les ascenseurs.

5. Chaque panneau de sécurité doit supporter un minimum de 8 lecteurs de justificatifs. Ces lecteurs doivent être en mesure de lire les données internes encodées dans chaque carte (ou le justificatif) puis d'envoyer ces informations au panneau de commande. Le panneau de commande doit traiter ces informations et ne déverrouillera le portail contrôlé approprié que si le justificatif est jugé valide.

6. Il doit être possible de configurer un portail du SSIE de SPPS pour la lecture des justificatifs d'identité sur « ENTRÉE » uniquement, et « ENTRÉE » et « SORTIE ».

7. Le SSIE de SPPS doit prendre en charge les lecteurs de justificatifs qui sont déployés sur le même système ainsi que le même panneau de commande. Le SSIE de SPPS doit prendre en charge les lecteurs de justificatifs suivants :
    i. lecteurs HID Wiegand compatibles avec le format de données Wiegand standard 26 bits;
    ii. HID iClass/Seos ou des capacités de cartes à puce semblables pour une expansion future;

   Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

8. Le SSIE de SPPS doit pouvoir définir un titulaire de justificatifs d'identité avec, au minimum, les champs ou attributs suivants :

    i. salutation (c'est-à-dire, Dr, M^{lle}, M., M^{me}, Professeur)
    ii. prénom;
    iii. deuxième prénom ou initiale (facultatif);
    iv. nom de famille;
    v. poste;
    vi. division;
    vii. type (p. ex., indéterminé, durée déterminée, occasionnel, étudiant, entrepreneur, visiteur, autre, etc.);
    viii. numéro d'appel direct;
    ix. numéro de cellulaire;
    x. numéro de carte interne;
    xi. numéro de carte externe (si différent);
    xii. NIP (caché et/ou visible);
    xiii. numéro de série de la carte (si mise en œuvre de cartes intelligentes);
    xiv. date d'activation;
    xv. date d'expiration;
    xvi. statut;
    xvii. groupe d'accès;
    xviii. photo;
    xix. modèle de carte d'identification avec photo;
    xx. signature;
    xxi. un minimum de 10 champs supplémentaires définissables par l'utilisateur;

xxii. date de modification du profil ou de l'identification de l'utilisateur et du poste de travail.

9. Comme le volume des modifications de justificatifs d'identité peut être très élevé, il est souhaitable que le SSIE de SPPS fournisse un moyen intuitif, efficace et efficient de créer, lire, mettre à jour et supprimer les enregistrements de justificatifs d'identité. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

10. Le SSIE de SPPS doit prendre en charge un NIP avec un minimum de 4 chiffres qui sont générés automatiquement par le SSIE de SPPS (et non sélectionnables par l'utilisateur). Les NIP doivent être cryptés dans la base de données et leur transmission aux panneaux de commande doit être cryptée.

11. Le SSIE de SPPS doit permettre aux utilisateurs disposant des autorisations appropriées d'interroger et de consulter les informations sur les titulaires de justificatifs d'identité à partir de n'importe quel poste de travail du SSIE de SPPS. Ces informations doivent comprendre tous les champs statiques et définis par l'utilisateur dans la fiche du titulaire de justificatifs d'identité.

12. Il ne doit pas être possible pour un administrateur ou un opérateur du système de consulter le NIP du titulaire de justificatifs d'identité, sauf autorisation, dont l'accès doit être strictement limité.

13. Le SSIE de SPPS doit générer, signalé et affiché les alarmes associées aux tentatives d'accès non valides (p. ex., mauvais horaire, justificatif d'identité non valide, aucun accès à ce lecteur/clavier, etc.).

14. Le temps de réponse entre la lecture de la carte (ou du justificatif) et le déverrouillage de la porte doit être inférieur à une seconde. Toutes les demandes d'accès doivent être traitées localement dans le panneau de commande pour une réponse plus rapide. En outre, la limite de temps d'ouverture de la porte et le délai de déverrouillage de la porte doivent être réglables par l'utilisateur avec un intervalle de temps allant de 1 à 255 secondes.

15. Chaque panneau de commande doit supporter les interrupteurs de sortie entièrement supervisés qui sont associés à chaque porte contrôlée par un lecteur. L'activation d'un interrupteur de sortie (bouton-poussoir, infrarouge passif ou barre anti-panique) doit libérer le dispositif de verrouillage et permet l'ouverture de la porte. La commande d'accès normale et la logique d'arrêt doit suivre l'activation de l'interrupteur de sortie. Chaque interrupteur de sortie doit être configuré, par l'entremise d'un logiciel, pour éteindre l'alarme associée ou pour couper l'alarme et déverrouiller la porte. Lorsque l'interrupteur de sortie est utilisé, le contact avec la porte connexe doit être désactivé afin d'éviter les fausses alarmes.

16. Si un panneau de commande détermine que le titulaire de justificatifs d'identité ne doit pas être autorisé à passer par une de ses portes associées, la porte doit rester verrouillée et une alarme de justificatif non valide doit être générée.

17. Le SSIE de SPPS doit supporter une fonction anti-retour de sorte que le système empêche l'utilisation répétée d'un justificatif à la même porte. Il est également souhaitable de soutenir une fonction d'accès refusé, un avis de violation d'anti-retour, et une règle d'anti-retour avec délai programmable.
    i. Une fonction d'accès refusé est défini comme une configuration logicielle qui interdit l'utilisation d'un justificatif valide sur un lecteur d'« ENTRÉE » à moins qu'il n'ait été utilisé sur le lecteur de « SORTIE » correspondant.
    ii. Un avis de violation d'anti-retour est défini comme une configuration logicielle qui permet l'utilisation d'un justificatif valide sur un lecteur d'« ENTRÉE » sans qu'il ait été utilisé sur le lecteur de « SORTIE » correspondant, mais qui présente un événement d'alarme lors d'une telle situation.
    iii. Un anti-retour avec délai programmable est défini comme une configuration logicielle qui interdit l'utilisation d'un justificatif valide sur un lecteur, à moins qu'une certaine période ne se soit écoulée depuis sa dernière utilisation sur le même lecteur.

18. Le SSIE de SPPS doit permettre la création et la définition de groupes d'accès qui définissent à quels lecteurs le titulaire de justificatifs d'identité (ou le groupe de titulaires) est autorisé à accéder, à quelles heures de la journée et quels jours de la semaine (ou jours congés). Les titulaires de justificatifs d'identité peuvent être regroupés au sein de groupes d'accès. Les lecteurs/claviers peuvent être regroupés en groupes d'accès. Il est souhaitable que la possibilité d'attribuer plusieurs horaires à un groupe d'accès soit possible. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

19. Aux fins du contrôle d'accès, le système doit prendre en charge un nombre illimité de groupes de vacances, chacun d'entre eux pouvant contenir jusqu'à 32 jours de congé. Il est souhaitable qu'un jour de congé soit défini en termes de jour de début et de fin. Les jours de congé peuvent être configurés comme jour de l'année, jour du mois, jour de la semaine et des combinaisons de ceux-ci, ainsi que des plages de dates discrètes. Chaque groupe de congé et chaque jour de congé doit porter un nom d'un maximum de 32 caractères. Il sera possible de configurer les congés et les groupes de congés comme des événements récurrents (hebdomadaires, mensuels ou annuels) et les événements de congés doivent être propres à un lieu et non à l'ensemble du système. Par conséquent, les congés peuvent être configurés pour un emplacement et ne pas avoir d'incidence sur ceux qui sont configurés pour un autre emplacement. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

20. Le SSIE de SPPS doit permettre de soutenir la définition de groupes d'accès avec, au minimum, les champs ou attributs suivants :
    i. nom du groupe d'accès;

ii. lecteurs et zones;
iii. horaires.

21. Le SSIE de SPPS doit prendre en charge les fonctions avancées de contrôle d'accès suivantes :
    i. groupes d'accès;
    ii. horaires;
    iii. congés;
    iv. exigences en matière d'accompagnateur;
    v. règles d'opération et opération prolongée pour les personnes handicapées;
    vi. expiration automatique du justificatif (date ou nombre d'utilisations).

22. Le SSIE de SPPS doit soutenir la création et la définition d'un nombre illimité de groupes d'accès temporaire. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

23. Afin de simplifier la saisie des données et les efforts nécessaires à l'administration du système de SSIE de SPPS, le logiciel doit fournir une méthode basée sur le comportement pour programmer les droits d'accès de chaque titulaire de justificatifs d'identité. Il est demandé que le SSIE de SPPS fonctionne comme suit :
    i. les lecteurs de justificatifs sont regroupés en zones, dont les noms sont conformes à leurs équivalents du monde réel (p. ex., portes d'enceinte, zone opérationnelle, zone de sécurité et zone de haute sécurité);
    ii. les zones et les horaires sont combinés par paires pour définir un concept logique appelé « groupe d'accès ». *Un groupe d'accès représente essentiellement plusieurs zones d'accès et d'horaires. La possibilité de nommer un groupe d'accès (p. ex., employés, entrepreneurs, personnel recruté sur place, etc.) permet de désigner le groupe d'accès en termes conventionnels, familiers à tous les utilisateurs du système, et qui sont utilisés au quotidien;*
    iii. en assignant chaque titulaire de justificatifs d'identité au groupe d'accès approprié, le système lui accorde automatiquement les droits d'accès à toutes les paires de zones d'accès et d'horaires définies pour ce groupe d'accès.

24. Le système doit être doté d'une fonction supplémentaire permettant d'appliquer des exceptions à tout titulaire de justificatifs d'identité ou groupe d'accès, de sorte qu'il ne soit pas nécessaire de créer de nouveaux groupes d'accès pour une seule ou un petit nombre d'exceptions (p. ex., un titulaire de justificatifs d'identité individuel ayant accès à une zone standard, mais n'ayant PAS accès à une zone particulière de cette zone). Les exceptions peuvent être basées sur les zones particulières incluses dans le groupe d'accès, ainsi que sur les horaires de fonctionnement de chaque zone particulière. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

    Remarque : si le fournisseur ne fournit pas d'exception installation, il est souhaitable qu'il décrive comment le système proposé permet une telle fonctionnalité d'une manière différente, éliminant ainsi la nécessité de définir des groupes d'accès supplémentaires pour

un (ou un petit nombre) de titulaires de justificatifs d'identité ayant des exigences d'accès précises.

25. Il est nécessaire que le SSIE de SPPS soutienne les capacités suivantes des groupes d'accès, des zones d'accès et des horaires :
    i. groupes d'accès : illimité;
    ii. zones d'accès : illimité;
    iii. horaires : illimité.

26. Le SSIE de SPPS doit soutenir la création et la définition d'un nombre illimité de groupes d'accès et d'horaires basés sur les rôles qui sont associés aux titulaires de justificatifs d'identité et aux zones ou secteurs pour lesquels le titulaire de justificatifs d'identité se voit accorder des privilèges d'accès.

27. Le SSIE de SPPS doit permettre de faire expirer un justificatif à une certaine date et à une certaine heure. Par ailleurs, il est souhaitable que le système prévoie une fonction permettant de définir un nombre précis de fois qu'un justificatif peut être utilisé. Cette définition doit être valable pour une utilisation de 1 à 999 fois depuis sa première utilisation (y compris la première fois qu'elle est utilisée). De plus, le système doit permettre de définir le nombre de jours, à partir de sa première utilisation ou de la date d'activation (l'une ou l'autre pouvant être sélectionnée), pendant lesquels le justificatif restera actif. Ces paramètres doivent s'échelonner de 1 à 999 jours. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

28. Le SSIE de SPPS doit fournir un certain nombre de fonctionnalités d'utilisation comme l'auto-remplissage, les éléments de menu déroulant, la personnalisation des étiquettes, la configuration de la disposition des fenêtres, les filtres, les facilités de recherche à entrée partielle et à champs multiples, et les champs pré-remplis pour faciliter la gestion des données et l'efficacité de l'administration du système. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

29. Le SSIE de SPPS doit prendre en charge le chargement en masse des données relatives aux titulaires de justificatifs d'identité (y compris les photos) à partir de systèmes ou de bases de données externes ou existants. Le système doit fournir des outils pour soutenir ce chargement de base de données. Si aucun outil n'est disponible, le transfert manuel des données est la responsabilité du fournisseur.

30. Le SSIE de SPPS doit prévoir une fonction d'accompagnement permettant de définir des étiquettes pour certains titulaires de justificatifs d'identité comme « accompagnement requis » et d'autres comme « accompagnant ». Dans cette configuration, il est souhaitable qu'un justificatif désigné comme « accompagnement requis » soit présenté à un lecteur, auquel cas le lecteur s'attendra à ce que l'accompagnant présente un justificatif au même lecteur. Une fois autorisé, la porte ou le portail doit être déverrouillé. Il est souhaitable que cette fonction puisse être assignée à un ou à tous les lecteurs du système et puisse être

activée pour une heure particulière en utilisant la même fonction de programmation horaire que celle utilisée ailleurs dans le système. Pour faciliter la saisie des données, il est souhaitable que le système utilise par défaut le titulaire « standard » de justificatifs d'identité, de sorte que tout titulaire de justificatifs d'identité nécessitant un accompagnant ou étant défini comme un accompagnant devra modifier discrètement la valeur par défaut. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

31. Le SSIE de SPPS doit prendre en charge une fonction de « fonctionnement étendu » grâce à laquelle l'administrateur peut modifier les temps de déverrouillage et de maintien de la porte par défaut pour les justificatifs désignés comme « fonctionnement étendu ». Cette fonction doit utiliser pour les portes ou portails d'assistance aux handicapés. Lorsqu'un justificatif autorisé désigné comme « fonctionnement étendu » est utilisé sur un lecteur particulier, s'il est configuré de la sorte, la porte doit s'ouvrir automatiquement, si elle est équipée d'un dispositif d'assistance à l'opérateur, et les temps de maintien et de déverrouillage de la porte prolongée sont demandés. Cette opération peut également être appliquée à un horaire.

32. Le SSIE de SPPS doit permettre le stockage de toutes les données relatives aux transactions, aux événements et aux alarmes de contrôle d'accès et de surveillance des alarmes d'intrusion pendant au moins deux ans. Ces événements doivent être stockés dans chacun des serveurs principaux.

SECTION K – GESTION DE L'IDENTIFICATION PAR PHOTO

1. Le système intégré de sécurité d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit permettre de créer, de gérer et de produire des cartes d'identification avec photo de manière totalement intégrée. Le sous-système de gestion des identifications par photo du SSIE de SPPS doit être une solution logicielle et matérielle entièrement intégrée pour la capture et le stockage d'images photographiques numérisées à haute résolution. Grâce à la base de données intégrée, toutes les données saisies dans la base de données des employés doit être immédiatement disponibles sur n'importe quel poste de travail du SSIE de SPPS.

2. Le SSIE de SPPS doit prendre en charge les appareils photo standard de l'industrie, les imprimantes de cartes, les tablettes de signature USB et tous les périphériques associés nécessaires au bon fonctionnement du sous-système de gestion des photos d'identité.

3. Tous les renseignements inclus dans le dossier du titulaire de justificatifs d'identité doivent être entièrement intégrés à la fonction d'identification avec photo. Les images vidéo haute résolution doivent être capturées, numérisées et stockées sur le disque dur local du poste de travail du SSIE de SPPS équipé pour la capture et l'inscription des titulaires de justificatifs d'identité avec photographies. Une fois l'image capturée, elle doit être traitée comme faisant partie de la base de données du SSIE de SPPS stockée dans les serveurs primaire et secondaire et pourra être appelée pour confirmation de l'identité visuelle sur tout autre poste de travail du SSIE de SPPS équipé d'un module d'imagerie vidéo, ou utilisée pour la

production et l'impression de cartes. Tout poste de travail du SSIE de SPPS doit pouvoir visualiser les photos des titulaires de justificatifs d'identité sans nécessiter de matériel particulier.

4. Le SSIE de SPPS doit soutenir la création, la gestion, la mise à jour et l'archivage de plusieurs modèles de conception d'identification avec photo. L'outil de conception de l'identification photographique doit prendre en charge la gestion des photos et des images de signature, sera entièrement intégré à la base de données de contrôle d'accès, fournira des outils et des éléments de dessin standard, permettra l'insertion et l'importation d'images de format standard, permettra la gestion des rapports d'aspect et le recadrage des images et prendra en charge plusieurs modèles et conceptions par titulaire de justificatifs d'identité. La carte doit être conçue en mode totalement interactif, avec un affichage en temps réel de sa forme actuelle pendant le processus. Il doit être également dessiné en utilisant le mode haute résolution du module d'affichage vidéo, pour une précision maximale et une reproduction fidèle des cartes finies. Chaque nouveau modèle de carte doit être stocké pour une récupération et une application rapides pendant la production de la carte d'utilisateur. Les cartes remplies doivent pouvoir être consultées à tout moment en haute résolution.

5. Le SSIE de SPPS doit prendre en charge la conception de cartes d'identification avec photo qui comprend des outils de conception graphique standard (lignes, cases, cercles, etc.), des motifs et des couleurs de lignes et de remplissage multiples, des tailles et des rapports d'aspect des photos contrôlés par l'utilisateur, des vues de face, vues de côté et des captures de signatures, l'accès à tous les champs de la base de données, des polices Windows standard, des graphiques statiques, un empilage d'objets contrôlé par l'utilisateur, des champs conditionnels de la base de données, diverses couleurs, d'autres éléments de sécurité (p. ex., des hologrammes), des signatures, des codes à barres, une impression recto verso et des fonctions de recadrage. Il est également nécessaire que le SSIE de SPPS prenne en charge une fonction permettant de verrouiller le rapport hauteur/largeur associé à la fenêtre de capture de la photo pour chaque modèle de carte. Il est nécessaire que le système fournisse également une fonction de recadrage pour permettre d'ajouter des photos à partir d'une base de données existante et de recadrer la photo pour qu'elle corresponde au format du nouveau modèle de carte. Décrivez comment le SSIE de SPPS proposé répond à chacune de ces exigences.

6. Le SSIE de SPPS doit prendre en charge les modèles existants d'imprimantes de cartes et de matériel photographique :

    - imprimante HID HDP5600;
    - caméra Web Logitech C920 1080P HD.

SECTION L – SURVEILLANCE ET CONTRÔLE DES ALARMES

1. Les alarmes doivent signalées et affichées sur un plan graphique ou dans une liste sur le poste de travail prédéfini du système intégré de sécurité d'entreprise de Sécurité publique Canada (SSIE de SPPS) dans les 2 secondes suivant le déclenchement du capteur.

2. Le SSIE de SPPS doit prendre en charge la connexion de divers dispositifs d'entrée d'alarme supervisés comme les interrupteurs de position de porte (contacts de porte), les détecteurs de mouvement, les détecteurs de bris de verre, les boutons de contrainte et autres dispositifs de signalisation semblables.

3. Pour les postes de travail des opérateurs du SSIE de SPPS configurés pour recevoir et traiter les alarmes, le système doit effectuer, dès réception d'une alarme, les opérations suivantes :

    i. afficher la ou les alarmes et activer un son auquel le gardien doit répondre;
    ii. afficher un plan graphique en couleur de la zone d'où proviennent la ou les alarmes, ou si l'opérateur le souhaite, présenter la ou les alarmes sous forme de liste. Les alarmes doivent être affichées par ordre de priorité;
    iii. afficher le nom du plan d'étage associé au point qui fait l'objet du rapport. L'affichage doit utiliser des icônes à code de couleur, superposées au plan de l'étage, pour indiquer l'emplacement réel de l'alarme. Des couleurs distinctes et différentes doivent représenter les éléments suivants : état d'alarme, état d'altération ou de défaillance, état de désactivation ou état de sécurité. Les couleurs doivent être définissables par l'utilisateur;
    iv. afficher une description complète de l'alarme et de l'état du point d'alarme;
    v. afficher la date et l'heure à laquelle le point d'alarme a été signalé pour la première fois;
    vi. archiver les renseignements sur l'événement d'alarme, y compris son état et la date et l'heure de l'événement sur les serveurs principaux et secondaires;
    vii. envoyer les renseignements techniques et l'alarme à un ou plusieurs appareils mobiles, le cas échéant;
    viii. envoyer les informations techniques et l'alarme au composeur du système, le cas échéant;
    ix. l'annonce des alarmes doivent avoir la priorité sur toute autre tâche en cours d'exécution; ces tâches doivent être suspendues jusqu'à la fin du traitement de l'alarme et doivent être ensuite rétablies au point avant l'interruption;
    x. si l'alarme est un événement lié à un justificatif et qu'une photo a été enregistrée pour ce titulaire de justificatifs d'identité, un bouton dans la barre d'outils doit demander l'ouverture d'une fenêtre qui doit afficheraà la photo, le nom et le numéro d'identification du titulaire de justificatifs d'identité, ainsi que le dernier lecteur consulté par ce titulaire de justificatifs d'identité;
    xi. en cas d'alarme sous contrainte, cette alarme doit être de la plus haute priorité et doit également affichée sur le poste de travail de gestion des identifications.

4. Au minimum, il doit être possible de définir, de configurer et de programmer les attributs suivants pour chaque entrée d'alarme ou d'événement :
    i. adresse technique de l'alarme ou de l'événement : les renseignements relatifs au point d'alarme doivent indiqués dans un formulaire qui décrit le numéro, le type, le type de module et le nom ou le numéro d'entrée du panneau de commande;
    ii. description de l'alarme ou de l'événement : le système doit permettre d'associer une description à chaque alarme.
    iii. priorité d'alarme : un numéro de priorité (de 1 à 16) défini par l'utilisateur doit être attribué aux alarmes afin de distinguer leur importance relative en cas d'alarmes multiples survenant simultanément;
    iv. les utilisateurs du groupe d'affichage du système doivent avoir la possibilité de désigner quel poste de travail du SSIE de SPPS ou quels groupes de postes de travail du SSIE de SPPS doit recevoir et afficher quelles conditions d'alarme. Jusqu'à 16 groupes de postes de travail de déclaration doivent être désignés et plusieurs postes de travail du SSIE de SPPS pourront être affectés à chaque groupe de déclaration. Un groupe doit être défini comme tout ensemble de postes de travail du SSIE de SPPS sur le réseau. Il doit être possible d'acheminer les alarmes pour afficher des groupes, quels que soient les profils d'utilisateurs ou les privilèges de connexion;
    v. définition de l'action de la caméra : le système doit être en mesure de relier une entrée d'alarme à une fenêtre contextuelle d'entrée de caméra de TVCF avec leurs fonctions associées de pivotement horizontal et d'inclinaison verticale, ainsi que de zoom préalablement réglées en fonction de la compatibilité des caméras. Ainsi, en cas d'alarme, le SSIE de SPPS doit être activé de manière à ce qu'une surveillance visuelle puisse être établie pour la zone de détection;
    vi. ensemble d'instructions ou instructions individuelles : chaque point d'alarme doit être être associé à un ensemble d'instructions de telle sorte que, en cas d'apparition d'une condition d'alarme, l'opérateur du système doit pouvoir le rappeler. Il doit être possible de créer et de modifier ces ensembles d'instructions à partir de n'importe quel poste de travail du SSIE de SPPS sur le réseau, à condition que l'opérateur ait le niveau d'autorisation approprié. Les rapports sur ces événements doivent être générés par le SSIE de SPPS;
    vii. type et couleur de l'icône d'indication : le système doit permettre d'associer différentes icônes à chaque alarme. Lorsque l'icône est sélectionnée pour correspondre à un point d'alarme, elle doit s'afficher sous forme graphique;
    viii. plan d'étage : le système doit fournir une fonction graphique à haute résolution pour l'affichage de plans et cartes en couleur en tant que norme afin d'aider les opérateurs à localiser et à répondre aux conditions d'alarme;
    ix. sorties liées : pour chaque point d'alarme, les utilisateurs doivent pouvoir relier des relais pour le contrôle des équipements. Pour chaque point d'alarme, les options d'actions liées doivent comprendre: verrouiller le relais et demander à l'opérateur de le réinitialiser à partir du site central; faire en sorte que le relais suive automatiquement l'état d'alarme, ou actionner le relais pendant une période déterminée après un changement d'état du point d'alarme;

x. programmes ou actions liés : pour chaque point d'alarme, les utilisateurs doivent pouvoir relier des programmes et des actions lorsqu'ils seront intégrés à des applications tierces et à des applications de TVCF;
xi. horaire : le système doit prévoir un minimum de 128 horaires. Chaque point d'alarme peut être affecté à l'un de ces horaires pour un aiguillage automatique;
xii. groupe d'alarme : un groupe d'alarme peut être une combinaison d'entrées. Les groupes doivent être présentés à l'opérateur sous la forme d'une icône unique afin de lui permettre d'effectuer des actions pour l'ensemble du groupe en tant que fonction unique. L'opérateur doit pouvoir également en mesure de manipuler les membres individuels du groupe;
xiii. alarme sonore : il doit être possible de définir un son d'alarme unique via un fichier de type .wav pour chaque entrée d'alarme. Le système doit être livré avec un son généré par ordinateur par défaut;
xiv. contrôle manuel : pendant le contrôle manuel, le système doit permettre à l'utilisateur d'inverser l'état actuel d'une entrée, d'un relais ou d'un groupe local.

5. Il est nécessaire que le SSIE de SPPS fournisse une capacité de gestion et d'affichage des alarmes pour signaler et afficher les alarmes sur un ou plusieurs postes de travail du SSIE de SPPS. Lors de l'affichage de l'alarme, les renseignements suivants, au minimum, doivent être fournis :
    i. le type d'alarme (illustré par une icône – p. ex., interrupteur de position de porte, détecteur de mouvement, alarme sous contrainte);
    ii. la date et l'heure de l'alarme (locale à ce panneau de commande);
    iii. description de l'alarme (en langage clair);
    iv. les détails techniques associés à l'alarme (adresse technique);
    v. affichage de l'alarme sur un plan d'étage ou dans une vue de liste (configurable);
    vi. alerte sonore de l'opérateur (personnalisable par alarme);
    vii. intégration de renseignements ou d'actions supplémentaires avec l'alarme ou appel de l'opérateur (vidéo, audio, photo de la personne associée avec justificatif, etc.);
    viii. alerte générée automatiquement (courriel ou SMS) (qui peut contenir un sous-ensemble des renseignements ci-dessus).

6. Il est souhaitable que le SSIE de SPPS prenne en charge le signalement et l'affichage des événements d'alarme sur des dispositifs d'affichage externes (mobiles) comme des téléphones intelligents et des téléphones portables. Pour de telles alarmes, il est souhaitable que le SSIE de SPPS fournisse les renseignements suivants dans son message à l'appareil mobile :
    i. type d'alarme
    ii. la date et l'heure de l'alarme (locale à ce panneau de commande);
    iii. description de l'alarme (en langage clair);
    iv. les détails techniques associés à l'alarme (adresse technique);
    v. alerte sonore intégrée.

Si le système proposé prend en charge cette fonctionnalité, décrivez comment le SSIE de SPPS proposé prend en charge cette exigence.

7. Pour chaque alarme ou événement dans le SSIE de SPPS, il doit être possible de définir un nom, un groupe d'alarme, une priorité, une action d'archivage, un ensemble d'instructions, un plan d'étage, une icône, un horaire, une capacité à contrôler l'alarme manuellement (c'est-à-dire, peut-elle être mise sous tension), l'emplacement de l'affichage lors de l'apparition, la programmation de la caméra, les sorties liées, les sons d'alarme, les groupes de destination de composeurs et des courriels.

8. Il doit être possible de signaler des alarmes à plusieurs endroits (ou destinations) simultanément ou séquentiellement, en fonction du type d'alarme ou de l'horaire.

9. Il doit être possible pour le SSIE de SPPS de soutenir l'utilisation de plans d'étage pour l'affichage des événements d'alarme. Un plan d'étage doit être automatiquement affiché à l'écran à chaque déclenchement d'alarme, à condition qu'il ait été préalablement spécifié d'utiliser cet affichage graphique. Le système doit prendre en charge une fonction de placement d'icônes selon le mouvement de la souris. Une fois que l'icône d'alarme a été placée sur la carte, l'administrateur du système peut la sélectionner et la placer n'importe où sur le plan. Le SSIE de SPPS doit prendre en charge l'importation de plans d'étage graphiques au format .bmp ou .jpg. Le SSIE de SPPS doit soutenir l'ajout des icônes des appareils notés comme des entités distinctes sur les plans d'étage.

10. Le SSIE de SPPS doit permettre de définir comment un utilisateur particulier, un groupe d'utilisateurs, un poste de travail ou un groupe de postes de travail accusent réception d'une alarme et l'effacent.

11. Il est nécessaire que le système supporte une fonction permettant de regrouper logiquement les entrées d'alarme en « groupes d'alarme ». Chaque groupe d'alarme doit être alors représenté dans le système par une seule icône qui pourra être agrandie pour montrer ses éléments. L'exploitant doit toujours avoir accès au contrôle de chaque élément du groupe et cette installation doit être utilisée pour mettre en œuvre des stratégies de zonage. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

12. Le SSIE de SPPS doit soutenir une installation pour l'activation de postures de sécurité où des zones particulières sont automatiquement verrouillées, armées, désarmées ou des actions semblables. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

13. Il doit être possible de relier n'importe quelle sortie du système à l'activation de n'importe quelle entrée du système de telle sorte que, lors de l'activation de l'entrée, le relais de sortie se verrouille, fasse des impulsions ou suit l'état de l'entrée d'alarme.

14. Tout administrateur du SSIE de SPPS doit avoir la possibilité de sélectionner et de contrôler manuellement toute sortie de relais dans le système. Une fois que l'icône représentant la

sortie a été sélectionnée, une fenêtre de contrôle apparaît et l'opérateur peut activer la sortie relais pendant une période définie par l'utilisateur.

15. Le système doit permettre de relier un point d'entrée d'alarme à un point de sortie numérique. Il doit être possible de désigner ce point de sortie comme étant soit à verrouillage, soit à impulsion, ou de suivre l'état du point d'entrée de l'alarme. Lors du verrouillage, le point de sortie numérique doit changer d'état et rester ainsi jusqu'à ce qu'il soit modifié par une commande de l'opérateur. En mode impulsion, le relais doit être activé pendant une période définie par l'utilisateur (0 à 8 000 secondes). En mode suivi, le point de sortie numérique change d'état au fur et à mesure que le point d'entrée de l'alarme change d'état.

16. Chaque point de sortie numérique peut être affecté à des horaires de sorte que les états des relais changent pendant la période déterminée. Cette fonction doit utilisée pour contrôler automatiquement les ascenseurs, les portes, les lumières, les portails et autres équipements.

17. Il doit être possible pour l'administrateur d'outrepasser manuellement ou de verrouiller un relais dans un état donné, l'empêchant ainsi de changer d'état jusqu'à ce qu'il soit déverrouillé manuellement, indépendamment de l'affectation des horaires ou des liens d'alarme en vigueur.

18. Il doit être possible pour un administrateur du SSIE de SPPS de définir un point de sortie, de sorte que chaque opération manuelle de ce point de sortie doit être reconnue par un « motif d'action » par l'opérateur du SSIE de SPPS avant qu'il ne réagisse. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

19. Le système doit prendre en charge une capacité de contrôle d'alarme locale pour l'armement et le désarmement des zones à l'aide des claviers de zone. Les zones peuvent être armées et désarmées localement ou à partir de n'importe quel poste de travail du SSIE de SPPS du réseau, selon les autorisations. Le clavier doit être basé sur un clavier matriciel à affichage standard de l'industrie. Il est également nécessaire que le système prenne en charge la configuration des entrées dans les zones qui doivent être contrôlées par le clavier de la zone ou par tout poste de travail du SSIE de SPPS sur le réseau. Il est également nécessaire que le système synchronise automatiquement les configurations d'entrée des alarmes locales entre la configuration d'alarme locale et la base de données du SSIE de SPPS. Le clavier doit afficher toutes les zones ouvertes, l'état du système, les conditions de panne et fournir une notification sonore pour l'armement et le désarmement de la zone. Le système doit également prendre en charge les programmes d'armement automatique. Par ailleurs, toutes les actions doivent être archivées et horodatées. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

SECTION M – GESTION VIDÉO

1. Pour l'instant, il n'est PAS nécessaire qu'un système de gestion vidéo (SGV) existant soit intégré au SSIE de SPPS, cependant le SSIE de SPPS doit être être en mesure d'intégrer la fonction de vidéo de façon transparente. Aucun matériel et logiciel de TVCF ne doit être remplacé, mais le contrat de service doit prévoir une couverture de service (section - S).

SECTION N – RAPPORTS DE GESTION

1. Le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit permettre l'archivage en temps réel de toutes les données historiques : transactions d'accès, événements d'alarme, images vidéo, activité du système, activité des opérateurs et des administrateurs, actions de gestion des données et modifications de configuration.

2. Le SSIE de SPPS doit soutenir un ensemble de rapports flexibles pour permettre la génération de données de rapport. Les fonctions du rapport doivent permettre de sélectionner rapidement et facilement divers champs à l'aide de menus déroulants. Il doivent permettre de répondre à des exigences communes et de créer des rapports personnalisés configurables par l'utilisateur.

3. Les rapports doivent être activés d'une ou de plusieurs des façons suivantes :
    i. initié par l'opérateur (manuel);
    ii. activation périodique à des intervalles spécifiés par l'utilisateur;
    iii. lancement d'une demande.

4. Le SSIE de SPPS doit offrir une méthode flexible et en temps réel pour les requêtes de données en ligne, à partir de n'importe quel endroit de l'application du SSIE de SPPS.

5. Le SSIE de SPPS doit alerté l'administrateur du système si sa capacité est limitée et si l'archivage de toutes les transactions et données est menacé.

6. Tous les rapports du SSIE de SPPS doivent être stockés dans la base de données du système et doivent pouvoir être consultés à partir de n'importe quel poste de travail d'opérateur ou d'administrateur du SSIE de SPPS et être contrôlés au moyen d'autorisations de système. Comme les données sont générées dans et depuis de nombreux fuseaux horaires, le système doit afficher les événements et les activités dans les rapports en fonction de leur heure locale et de cette heure archivée dans la base de données des transactions du système. Le SSIE de SPPS doit permettre à l'utilisateur d'exporter des rapports basés sur les événements du système ou selon un horaire défini par l'utilisateur.

7. Le SSIE de SPPS doit fournir une base de données et des rapports d'archives et de transactions. Le système doit être livré avec un certain nombre de bases de données et de rapports d'archives et de transactions standard, qui couvrent les renseignements les plus fréquemment demandés.

8. La configuration des rapports de gestion ne nécessitera que la saisie des renseignements relatifs à l'horaire et d'autres paramètres comme le titulaire de justificatifs d'identité, le nom de l'alarme ou de l'événement, les renseignements de filtre ou l'intervalle de temps de recherche pour configurer entièrement le rapport. Aucune programmation et aucun script ne doit être nécessaire.

9. Il est nécessaire que le SSIE de SPPS soit livré avec les rapports standard suivants disponibles dans le système :
    i. utilisateurs du système et privilèges;
    ii. administrateurs;
    iii. opérateurs;
    iv. personnel technique;
    v. titulaires de justificatifs d'identité (y compris tous les champs ou un sous-ensemble de tous les champs de chaque enregistrement);
    vi. groupes d'accès, niveaux;
    vii. transactions d'événements du système;
    viii. tentatives d'accès valides et non valides;
    ix. alarmes et événements, y compris les accusés de réception et les réponses;
    x. activités et violations de l'anti-retour;
    xi. événements liés aux alarmes et vidéos;
    xii. événements prévus;
    xiii. matériel du système;
    xiv. serveurs, postes de travail;
    xv. panneaux de commande;
    xvi. modules du panneau de commande;
    xvii. lecteurs, portes, portails;
    xviii. entrées d'alarme;
    xix. sorties de relais;
    xx. caméras;
    xxi. configurations du système;
    xxii. groupes d'accès, niveaux;
    xxiii. groupes et zones d'alerte;
    xxiv. congés, horaires;
    xxv. configurations anti-retour.

10. Décrivez comment le SSIE de SPPS proposé répond à ces exigences.

11. Le SSIE de SPPS doit pouvoir exporter manuellement et automatiquement (ou d'envoyer à un lecteur) les rapports dans chacun des formats suivants : .pdf, .txt, .doc et .xls. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

12. Le SSIE de SPPS doit fournir une capacité d'audit des modifications de la base de données. Pour chaque modification de champ dans la base de données, il est souhaitable que le système archive et affiche, en temps réel (et permette de faire des rapports à l'avenir), la date de modification, le nom de connexion, le nom du tableau, le contexte, le type de modification (insertion, modification, suppression), le nom du champ, l'ancienne valeur, l'ancien contexte, la nouvelle valeur et le nouveau contexte. Il est souhaitable que tous les changements soient horodatés à la seconde près. Décrivez comment le SSIE de SPPS proposé répond à cette exigence.

13. Il est nécessaire que le SSIE de SPPS fournisse des capacités d'examiner et de suivre tous les rapports générés sur le système aux utilisateurs qui sont des administrateurs.

SECTION O – DOCUMENTATION

1. La documentation suivante sur le système de sécurité intégrée d'entreprise de Sécurité publique Canada (SSIE de SPPS) doit être fournie au moment de la soumission de la proposition, sous forme électronique et sur papier, en anglais uniquement. SP/PS prendra les dispositions nécessaires pour la traduction des produits livrables produits par l'entrepreneur, au besoin.

    i. Manuels de configuration : les manuels de configuration doivent comprendre des descriptions relatives aux plateformes de contrôle d'accès et de TVCF et à leurs paramètres de configuration technique, en mettant l'accent sur les serveurs principal primaire et secondaire, les enregistreurs vidéo en réseau et les appareils, les logiciels des panneaux de commande, les paramètres du matériel et des réseaux et les procédures d'installation. Ces manuels doivent porter au minimum sur les serveurs du SSIE de SPPS, les postes de travail du SSIE de SPPS, le système d'exploitation, le réseau, la base de données, la définition et la gestion des ports, le fonctionnement des services, les communications, les modules de panneaux de commande, les caméras et les dispositifs de stockage du système vidéo et la mise en œuvre des composants de la tête de réseau du SSIE de SPPS.

    ii. Manuels d'utilisation : les manuels d'exploitation doivent comprendre des descriptions relatives au fonctionnement du système, en mettant l'accent sur la surveillance, la notification et la gestion des alarmes, ainsi que sur les fonctionnalités intégrées du système généralement assurées par les opérateurs du système (p. ex., les gardes, les équipes de surveillance). Au minimum, ces manuels doivent traiter des postes de travail du SSIE de SPPS, des procédures de démarrage et de connexion au système, des procédures d'arrêt et de déconnexion du système, de l'utilisation du système et des commandes et logiciels associés, de la surveillance et de la gestion des alarmes, de la surveillance vidéo, des fonctionnalités du système intégré, de la génération de rapports, de la saisie de données, des commandes de navigation de l'opérateur, des descriptions et actions d'alarme et des exigences de sécurité du système.

    iii. Manuels de l'administrateur : les manuels de l'administrateur doivent comprendre des descriptions des fonctions de tous les modules du logiciel et doit inclure tous les autres renseignements nécessaires pour gérer efficacement le SSIE de SPPS. Le manuel de l'administrateur doit traiter de la configuration et de la gestion du logiciel d'application du SSIE de SPPS et de chacun de ses modules respectifs. Au minimum, le

manuel de l'administrateur doit donner un aperçu de l'application du SSIE de SPPS, un examen de tous les outils courants de l'interface utilisateur (p. ex., ajouter/supprimer/modifier des données, fonctions de recherche et de localisation, vues et filtres des données, barres d'outils et menus) et une aide à la planification des paramètres du système. Au minimum, le manuel de l'administrateur doit traiter des éléments suivants : profils d'utilisateurs de l'application du SSIE de SPPS, privilèges et paramètres de contrôle d'accès, gestion de la base de données des titulaires de justificatifs d'identité, groupes d'accès, horaires, zones, titulaires de justificatifs d'identité, définitions des systèmes d'alarme, paramètres de gestion des systèmes vidéo, configuration et programmation du système de gestion des visiteurs, configuration et programmation du système d'identification par photo, intégration des sous-systèmes (p. ex., Active Directory), et archivage et rapports de gestion.

iv. Manuels d'installation : les manuels d'installation doivent comprendre des descriptions sur les méthodes appropriées et les pratiques exemplaires pour l'installation des produits matériels du fournisseur et des appareils et composants associés sur le terrain, y compris l'établissement de modes de communication. Au minimum, ces manuels doit fournir une description générale du système, de plans «as built», du matériel et des composants et traiteront des procédures d'installation, de la disposition des équipements et des schémas électriques, des besoins en énergie, de la disposition et des schémas du système, ainsi que des pièces de rechange et de réparation.

v. Manuels d'entretien : les manuels d'entretien doit comprendre des descriptions de l'entretien, de l'assistance, du dépannage et des instructions de service pour tous les équipements et les modules logiciels applicables. Au minimum, ces manuels doit traiter de l'inspection, de l'entretien préventif, du diagnostic des défaillances ainsi que des procédures de réparation et de remplacement.

2. Par ailleurs, le SSIE de SPPS doit contenir une aide en ligne contextuelle pour aider les utilisateurs du SSIE de SPPS dans la configuration et le fonctionnement du SSIE de SPPS. Les menus d'aide doivent être accessibles à partir de n'importe quelle fenêtre du SSIE de SPPS en cliquant sur une icône toujours présente à la même position de l'écran ou en appuyant sur une touche de fonction précise. Les fenêtres d'aide doivent être sensibles au contexte, de sorte que les utilisateurs du système puissent passer d'une fenêtre à l'autre sans quitter la fenêtre d'aide. Les commandes d'aide standard de Windows pour le contenu, la recherche, le retour et l'impression doivent également être disponibles.

3. Dans le cadre de sa soumission, le fournisseur doit également inclure une copie séparée des fichiers de documentation en ligne complets dans un format électronique facilement accessible tel que les fichiers .pdf ou .doc. Décrivez comment le fournisseur respecte cette exigence.

4. Le fournisseur du SSIE de SPPS est tenu de donner accès à ses outils et mécanismes de soutien, notamment, mais pas exclusivement, aux notes de mise à jour, aux notes techniques, aux avis de modification technique, aux listes de bogues, aux listes de problèmes en suspens, aux forums de soutien en ligne, aux groupes d'utilisateurs et aux mécanismes de demande de fonctionnalités et de nouvelles capacités. Décrivez comment le fournisseur respecte cette exigence.

SECTION P – LISTE DES PIÈCES MAÎTRESSES

Les fournisseurs doivent :

1. Fournir une liste des principale pièces de tous les composants, y compris les composants tiers qui seraient nécessaires pour construire un système de sécurité intégrée d'entreprise pour Sécurité publique Canada (SSIE de SPPS) incluant les composants et les logiciels des fournisseurs et des tiers.

2. Le tableau de la liste des pièces maîtresses doit comprendre tous les éléments énumérés dans la section R.

3. Le tableau de la liste des pièces maîtresses doit comprendre des pièces supplémentaires, selon les besoins, pour un SSIE de SPPS entièrement fonctionnel.

4. Il est à noter que les exigences détaillées ne sont pas fournies pour les dispositifs de sécurité comme les interrupteurs de position des portes, les capteurs d'alarme, les serrures de porte, les sondeurs piézoélectriques, etc. Le fournisseur peut proposer de tels produits pour appuyer une mise en œuvre complète du SSIE de SPPS.

5. Le SSIE de SPPS doit être compatible et prendre en charge les produits énumérés dans la liste de la section R.

SECTION Q – RESSOURCES POUR LES FOURNISSEURS

SP/PS a besoin du soutien des ressources du fournisseur pendant les diverses étapes d'installation du système. Le fournisseur doit fournir au moins une ressource conforme dans chacune des catégories de ressources incluses dans cette section.

Il est nécessaire que le fournisseur offre une option pour un délai de réponse garanti de quatre heures pour tous les (2) sites situés dans la région de la capitale nationale dans le cadre de la proposition.

Le fournisseur doit fournir les coordonnées de chacune des ressources pour chaque emplacement mentionné, à moins d'indication contraire pendant l'exécution des travaux, en donnant un préavis minimal de 24 heures des personnes qui travailleront et de l'endroit où les travaux auront lieu. Chaque ressource doit être un employé direct du fournisseur, aucune entreprise tierce ne doit être utilisée, sauf s'il s'agit de métiers spéciaux tels que les électriciens et les serruriers. Chaque ressource doit inclure, au minimum : le nom complet, le lieu de travail, le niveau d'habilitation de sécurité et les numéros de dossier, les descriptions de projet et de rôle, les certifications de l'industrie et du produit (y compris les certifications sur le produit proposé).

Le fournisseur doit proposer des ressources qui satisfont ou dépassent les exigences suivantes :

1. **Architecte du système** : un expert en la matière ayant une connaissance et une expérience approfondies du système et de la conception de l'infrastructure de base. Autorisation de sécurité (niveau **FIABILITÉ**).

2. **Gestionnaire de projet :** un gestionnaire de projet ayant une grande expérience de la structure de répartition des tâches et du processus de conception et de mise en œuvre d'un nouveau système de base et de transition à partir d'un système existant. Autorisation de sécurité (niveau **FIABILITÉ**).

3. **Technicien en matériel informatique :** un technicien possédant une vaste expérience et une grande compétence dans la mise en œuvre, la mise à l'essai et la mise au point du nouveau matériel et des nouveaux logiciels du système de base. Autorisation de sécurité (niveau **FIABILITÉ**).

4. **Responsable technique des logiciels d'application :** un responsable technique des logiciels d'application qui possède l'expérience et les compétences nécessaires pour mettre en œuvre, mettre à l'essai et mettre au point les applications et les logiciels de tiers pour le système de base et les postes des utilisateurs. Autorisation de sécurité (niveau **FIABILITÉ**).

5. **Formateur** : un formateur bilingue (français et anglais canadien) ayant une expertise en la matière et une expérience dans la formation d'administrateurs de systèmes, d'opérateurs, d'installateurs et de personnel d'entretien du SSIE de SPPS. Le bilinguisme signifie la maîtrise de l'écrit et de l'oral dans les deux langues. Cela doit être démontré à l'aide de certificats d'enseignement particuliers ou d'accréditations de fabricants et d'années d'expérience. Actuellement, SP/PS exige un minimum de (6) employés formés à l'utilisation du système. Autorisation de sécurité (niveau **FIABILITÉ**).

Le fournisseur doit offrir tous les services requis dans ce document aux endroits suivants :

- Burnaby (Colombie-Britannique)
- Edmonton (Alberta)
- Regina (Saskatchewan)
- Winnipeg (Manitoba)
- Fredericton (Nouveau-Brunswick)
- Toronto (Ontario)
- Ottawa (Ontario)
- Montréal (Québec)
- Dartmouth (Nouvelle-Écosse)
- Charlottetown (Île-du-Prince-Édouard)
- St. John's (Terre-Neuve-et-Labrador)

SECTION R – SITES MINISTÉRIELS ET EXIGENCES EN MATIÈRE DE MATÉRIEL

Afin de faciliter la proposition du fournisseur, voici une brève description des besoins en matériel pour chaque site. On y indique également les composants qui sont déjà installés et qui devraient rester, sauf indication contraire, et qui doivent s'intégrer et fonctionner partiellement ou entièrement avec le système proposé.

<u>Remarque importante</u> Le fournisseur doit être responsable de la coordination, de l'installation, de la fourniture du matériel, de la programmation, des essais et de la mise en service des deux sites indiqués ci-dessous.

1. 269, avenue Laurier, Ottawa (Ontario) – administration centrale et centre des opérations de sécurité, comprenant jusqu'à 13 étages.

Existant;

– 247 lecteurs de cartes et matériel de porte associé;
– 90 claviers anti-intrusion (intégrés au SCA);
– jusqu'à 874 entrées au total du système – chaque panneau de contrôle d'accès possède 12 entrées et 12 sorties intégrées;
– jusqu'à 294 sorties au total du système – chaque panneau de contrôle d'accès possède 12 entrées et 12 sorties intégrées;
– 59 groupes d'accès;
– 19 horaires;
– 2480 titulaires de cartes;
– 90 zones;
– 1 serveur de contrôle d'accès;
– 3 postes de travail de clients avec contrôle d'accès.

Responsabilité du fournisseur – nouvelle installation; (fourniture et installation ou remplacement)

– Remplacer 238 lecteurs de cartes par des lecteurs HID Multiclass SE (R40)
– Remplacer 9 lecteurs de cartes à clavier par des lecteurs HID Multiclass SE (RK40)
– Remplacer 17 panneaux de contrôle d'accès pour remplacer les composants électroniques du contrôleur automatique

– Remplacer 113 contrôleurs de porte simple pour remplacer l'appareil de contrôle de redondance cyclique (CRC)
– Remplacer les tableaux de 39 entrées par 16 entrées par tableau
– Remplacer 90 claviers d'intrusion pour du matériel KP-DISP
– Installez 17 alimentations 12 V CC (Altronix AL600ULX ou équivalent)
– Remplacer 17 alimentations 24 V CC (Altronix AL600ULX ou équivalent)
– Installer 1 support monté d'ASI pour serveurs (Eaton 9PX1500RT avec Eaton 9PXEBM48RT ou équivalent)
– Installer 1 API pour le poste de travail du CSO uniquement (Eaton 5S1000LCD ou équivalent)
– Installer tout contrôle d'accès local en amont ou en aval de la communication (si nécessaire)

2. 340, avenue Laurier, Ottawa (Ontario)

Existant;

– 44 lecteurs de cartes et matériel de porte associé;
– jusqu'à 284 entrées au total du système;
– jusqu'à 124 sorties du système;
– 59 groupes d'accès;
– 90 zones;
– 1 poste de travail client avec contrôle d'accès.

Responsabilité du fournisseur – nouvelle installation; (fourniture et installation ou remplacement)

– Remplacer 34 lecteurs de cartes par des lecteurs HID Multiclass SE (R40)
– Remplacer 10 lecteurs de cartes à clavier par des lecteurs HID Multiclass SE (RK40)
– Remplacer 4 panneaux de contrôle d'accès pour remplacer le matériel de TIC
– Remplacer les tableaux de 5 entrées par 16 entrées par tableau
– Remplacer 4 claviers anti-intrusion pour remplacer le matériel de TIC
– Installer 4 alimentations 12 V CC (Altronix AL600ULX ou équivalent)
– Remplacer 4 alimentations 24 V CC (Altronix AL600ULX ou équivalent)
– Installer tout contrôle d'accès local en amont ou en aval de la communication (si nécessaire)

SECTION S – ENTENTE DE SERVICE

Aperçu

Le fournisseur doit fournir tous les logiciels et les services de soutien des solutions intégrées pour Sécurité publique Canada (SSIE de SPPS) dans la RCN. Le fournisseur doit fournir

Portée des travaux

1. Le fournisseur doit fournir;
   – un point de contact unique pour les questions d'assistance et d'entretien en cours;
   – un accès à un service d'assistance technique par téléphone;
   – un soutien et un entretien continus des modules d'intégration personnalisés conçus pour les intégrations d'Active Directory;
   – un accès à un nombre illimité de mises à jour et de mises à niveau de logiciels (logiciels uniquement); SP doit avoir accès à toutes les dernières versions de logiciels, mises à niveau, correctifs et rustines de bogues de chaque sous-système. Le fournisseur comprend que les mises à jour et les mises à niveau des logiciels ne seront mises en œuvre qu'après approbation du système de production. SP/PS et le fournisseur doivent travaillé en collaboration pour établir un calendrier de qualification et de mise en œuvre de nouveaux logiciels;

– Fournir des mises à jour, des correctifs et une assistance au système d'exploitation des serveurs et à toutes les applications tierces requises dans la section D.;

– de l'assistance à l'élaboration de politiques et de procédures permettant le rétablissement ou la poursuite de la solution du SSIE de SPPS dans les situations d'urgence (naturelles ou provoquées par l'homme).

2. Un ingénieur de soutien à plein temps (du lundi au vendredi, de 8 h à 17 h) doit être mis à la disposition de SP/PS sur demande, et cette personne doit être responsable des activités suivantes :

a. fournir une expertise sur place pour la solution du SSIE de SPPS sur demande et agir en tant que premier point de contact pour toute question liée à la solution du SSIE de SPPS;
b. suivre et gérer tous les billets liés au soutien des services émis par les systèmes de SP pour la solution du SSIE de SPPS et effectuer une analyse des causes profondes de chaque problème depuis l'administration centrale, si nécessaire;
c. fournir des formations de mise à jour aux employés et techniciens des services de sécurité électronique de SP/PS sur les principales mises à jour de contenu, les mises à niveau de logiciels et l'ajout de nouveaux ensembles de caractéristiques et de fonctionnalités;
d. suivre et gérer l'état de la garantie des composants de la solution, initier et gérer les demandes de garantie auprès de chaque fournisseur et s'assurer de la résolution.

3. Le fournisseur doit offrir un accès à un centre d'appel pour les appels de service disponibles en permanence sans avoir à recourir à des services de réponse de tiers. Pour garantir une réponse de qualité, le fournisseur doit garantir un temps de réponse de 2 heures pendant les heures normales d'ouverture (du lundi au vendredi de 8 h à 17 h) et de 4 heures après les heures de bureau par un technicien de la région de la capitale nationale.

SECTION T – PRODUITS LIVRABLES PAR LE FOURNISSEUR

1.1 Lors de l'attribution du contrat et avant toute exécution de travaux, le fournisseur doit fournir l'approche et la méthodologie proposées en détail pour réussir la migration et le passage au système de sécurité intégré d'entreprise avec soin.

1.2 Les rapports sur l'état d'avancement des activités achevées, actives et à venir, les écarts par rapport au calendrier et au budget, les problèmes et risques avec les réponses proposées, ainsi que les demandes de changement proposées doivent être présentés chaque semaine pendant la durée du contrat.

1.3 Tous les services fournis par l'entrepreneur dans le cadre du contrat doivent, au moment de l'acceptation, être exempts de défauts de fabrication et être conformes aux codes applicables. Si l'entrepreneur doit corriger ou remplacer le travail ou une partie des travaux, il doit n'en coûter rien au gouvernement du Canada.

1.4 Tous les travaux doivent être effectués dans les installations de Sécurité publique Canada à Ottawa (Ontario) et se doivent se dérouler pendant les heures normales de travail du lundi au vendredi, de 8 h à 17 h. Dans les zones de sécurité de haut niveau, les travaux pourraient se dérouler entre 18 h et 6 h avec un accompagnant (avis de 48 heures).

1.5 Toutes les communications avec le personnel de Sécurité publique Canada et le public canadien (*le cas échéant*) doivent être effectuées dans la langue officielle (*anglais ou français*) préférée par l'employé ou le citoyen.

1.6 Tous les produits livrables doivent être présentés en anglais.

1.7 SP/PS prendra les dispositions nécessaires pour la traduction des produits livrables produits par l'entrepreneur, le cas échéant.

1.8 Les travaux doivent être exécutés conformément aux lignes directrices de chaque groupe de gestion du bâtiment ou de SPAC et aux codes ou normes locales applicables en vigueur au début de l'installation. La liste suivante résume les normes applicables :

i. norme UL 294 (Access Control Units);
ii. norme UL 294B (Power Over Ethernet (PoE) Power Sources for Access Control Systems and Equipment);
iii. norme UL 302 (Installation, inspection and testing of intrusion alarm systems);
iv. norme LAC 304 (Signal Receiving Centre and Premise Burglar Alarm Control Units);
v. norme UL 1076 (Proprietary Burglar Alarm Units and Systems).

SECTION U – SOUTIEN À SP/PS

Selon les besoins de l'exécution du travail contractuel et à la discrétion de l'autorité technique ou de l'autorité de projet de SP/PS, SP/PS s'efforcera de fournir au personnel de l'entrepreneur :

i. la documentation interne pertinente;
ii. des bureaux sur place dans les installations de Sécurité publique Canada à Ottawa (*si d'autres dispositions sont nécessaires, elles seront prises par l'autorité technique du projet de SP*);
iii. un accès programmé aux installations;
iv. des examens, de la rétroaction et des approbations des résultats en temps utile.

SECTION V – EXPANSION FUTURE

SP/PS opère dans de nombreux bureaux régionaux au Canada et la vision à long terme est d'intégrer ces bureaux à la nouvelle plateforme du système. Bien que le service et l'installation pour les bureaux régionaux de SP à l'extérieur d'Ottawa (ON) ne soient pas une exigence dans le cadre de cette phase, le soumissionnaire doit avoir la capacité de fournir l'installation et les services dans les villes énumérées dans la section Q pour les autorisations de tâches futures.

La majeure partie du projet sera complétée dans la phase 1 (340 Laurier et 269 Laurier). Le nombre d'employés par bureau régional varie entre 1 et 30 employés par emplacement, donc le travail futures dans les bureaux régionaux devraient être un ajout mineur au système mis en œuvre dans la phase 1.

La nature et l'étendue exactes des travaux pour les besoins des bureaux régionaux seront déterminées ultérieurement, lorsque les besoins et les lieux seront connus.

(Fin de page)

ACRONYMES et ABRÉVIATIONS

AD	Active Directory	SCOM	Microsoft System Center Operations Manager
AES	Norme de chiffrement avancé (AES)	SCOM	Microsoft System Center Operations Manager
API	Interface de programmation d'applications	PTR	Protocole de temps du réseau
ASIS	ASIS International (American Society for Industrial Security)	EVR	Enregistreurs vidéo en réseau
SSIE de SPPS	Système de sécurité intégrée d'entreprise de Sécurité publique/Public Safety		
SP/PS	Sécurité publique/Public Safety Canada	O/S	Système d'exploitation
CPP	Certified Protection Professional	PTZ	Fonctions de pivotement horizontal, d'inclinaison verticale et de zoom
TVCF	Télévision en circuit fermé	PS	Public Safety Canada
TVCF	Système de télévision en circuit fermé	SPC	Sécurité publique Canada
ILC	Interface de ligne de commande	NIP	Numéro d'identification personnel
SCPE	Solutions commerciales prêtes à l'emploi	PSP	Professionnel de la sécurité physique
CST	Centre de la sécurité des télécommunications	PoE	Alimentation électrique par Ethernet
SGVN	Système de gestion vidéo numérique	QS	Qualité de service
EVN	Enregistreur vidéo numérique	IRF	Identification par radiofréquence
		C	Coté
SVN	Système vidéo numérique	GRC	Gendarmerie royale du Canada
DNS	Système de nom de domaine	SMTP	Protocole de transfert de courrier simple
DHCP	Protocole de configuration d'hôte dynamique	SNMP	Protocole de gestion de réseau simple
FDL	Fin de ligne	IU	Identification unique
FTP	Protocole de transfert de fichiers	SDK	Trousse de développement de logiciel
CVC	Chauffage, ventilation et climatisation	SAN	Réseau de stockage de données
HTTP	Protocole de transfert hypertexte	TCP/IP	Protocole de contrôle de transmission/Protocole Internet
TI	Technologie de l'information	TFTP	Trivial File Transfer Protocol
TI/GI	Technologies de l'information/Gestion de l'information	UL/LAC	Underwriters Laboratories/Laboratoires des assureurs du Canada
ISO	Organisation internationale de normalisation	ASI	Alimentation sans interruption
IP	Protocole Internet	VSAT	Microstation terrienne
O	Obligatoire		
DFSR	Réplication du système des fichiers distribués de Microsoft	LGV	Logiciel de gestion vidéo

ANNEXE B **Demande de propositions** **Modernisation du contrôle d'accès**

Nom de l'entreprise :

Nom des ressources :

Signatures :

_____		_____	
Évaluateur	Date	Contracting	Date
_____		_____	
Évaluateur	Date	Évaluateur	Date

REMARQUE

Respecte tous les critères obligatoires : OUI? _____NON? _____

Note maximale disponible : 15

Total des points obtenus : _____

N° de la DOC :

CRITÈRES D'ÉVALUATION OBLIGATOIRES

Critères	Critère	Respecté/non respecté Commentaires
O1	Le soumissionnaire doit proposer un **Gestionnaire de Projet**. Le soumissionnaire doit aussi proposer une équipe de ressources nécessaires et leur rôle dans le projet qui permettra l'achèvement des travaux requis énumérés dans l'énoncé des travaux. Pour les ressources proposées, le soumissionnaire doit présenter un curriculum vitæ (CV) détaillé qui décrit clairement les projets pertinents de l'expérience professionnelle de la ressource. (Au moins cinq [5] ans directement liés à l'intégration des systèmes de sécurité et aux installations sur les systèmes de sécurité d'entreprise) Le soumissionnaire doit mettre en caractère gras ou en évidence les domaines pertinents dans le CV de la ressource. Au minimum, le soumissionnaire doit fournir les renseignements suivants sur le CV : • nom complet de la personne proposée; • formation/qualification scolaire; • expérience professionnelle pertinente et la durée de chaque projet.	
O2	Le soumissionnaire doit démontrer que l'équipe de ressources proposée a travaillé dans l'industrie de la sécurité, a offert des services de sécurité de taille et de portée semblables aux services décrits dans l'énoncé des travaux (planification, mise en œuvre, entretien, réparation, mise à niveau de la gestion des accès, alarme d'intrusion et installation d'un système de sécurité intégré d'entreprise) au cours des dix (10) dernières années. Le soumissionnaire doit indiquer au moins trois (3) projets de taille et d'envergure semblables au cours des cinq (5) dernières années. Pour chaque projet, le soumissionnaire doit fournir, au minimum, les	

N° de la DOC :

Critères	Critère	Respecté/non respecté Commentaires
	renseignements suivants : • nom du client; • description du projet; • détermination et rôle de la ressource dans le cadre du projet; • date et durée du projet; • justification de la manière dont le projet répond au critère.	
O3	Le soumissionnaire doit fournir des documents **signés** par son fournisseur ou fabricant qui prouvent qu'il est autorisé à recevoir une assistance technique et qu'il est en mesure d'acheter du matériel et des logiciels auprès du fournisseur ou du fabricant. Les documents signés doivent figurer sur un papier à en-tête du fournisseur ou du fabricant.	
O4	Le soumissionnaire DOIT démontrer que l'équipe de ressources proposée a **dirigé** un minimum de cinq (5) projets liés aux **systèmes de contrôle d'accès du gouvernement** au cours des dix (10) dernières années, dans lesquels les ressources proposées ont planifié, conçu, mis en œuvre et achevé le projet avec succès. Pour chaque projet, le soumissionnaire doit fournir, au minimum, les renseignements suivants : • nom du client; • description du projet; • détermination et rôle des ressources dans le cadre du projet; • date et durée du projet; • justification de la manière dont le projet répond au critère. Une ou plusieurs des ressources proposées peuvent être utilisées pour respecter ce critère.	

LE NON-RESPECT PAR LE SOUMISSIONNAIRE DE TOUS LES CRITÈRES D'ÉVALUATION OBLIGATOIRES ENTRAÎNE UNE DÉTERMINATION DE NON-CONFORMITÉ ET LA SOUMISSION NE FERA PAS L'OBJET D'UNE ÉVALUATION PLUS APPROFONDIE.

N° de la DOC :

CRITÈRE D'ÉVALUATION COTÉS

Les offres qui satisfont à tous les critères techniques obligatoires seront évaluées et notées comme spécifié dans les tableaux insérés ci-dessous. **Le soumissionnaire doit fournir suffisamment de détails pour démontrer clairement comment il satisfait à chaque exigence cotée ci-dessous. Les soumissionnaires sont avisés que la seule énumération de l'expérience sans fournir de données et d'informations à l'appui pour décrire les responsabilités, les fonctions et la pertinence par rapport aux exigences, ou en réutilisant le même libellé que la DP, ne sera pas considérée comme «démontrée» aux fins de la présente évaluation.**

R1 – Le **Gestionnaire de Projet** proposé par le soumissionnaire sera évalué en fonction de ses années d'expérience en matière d'installation de systèmes de contrôle d'accès de taille, d'échelle et de complexité similaires.

5 points seront attribués pour chaque année supplémentaire d'expérience de projet de taille et de portée similaires (après 5 ans d'expérience obligatoire identifié à M1). (15 points max.)

Total maximum de points techniques R1	**15 points**
Total des points R1 reçus	

COMMON-PS-SRCL#2

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
Security Classification / Classification de sécurité UNCLASSIFIED	

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Public Safety Canada	Corporate Management Branch
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Public Safety / Sécurité publique Canada (PSSP) National Headquarters in the National Capital Region currently has a requirement to upgrade their legacy Access Control/ Intrusion System. The current legacy systems are based on 1. Summit Enterprise eNT and 2. ICT Protégé System. The requirement is to upgrade to a centralized modern Enterprise Integrated Security System with which to protect, defend and respond to actual and potential security and life-safety events and situations affecting its people, assets and information.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☑ No / Non	☐ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☐ No / Non	☑ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☐	NATO / OTAN ☐	Foreign / Étranger ☐

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions Aucune restriction relative à la diffusion ☐	All NATO countries Tous les pays de l'OTAN ☐	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A PROTÉGÉ A ☐	NATO UNCLASSIFIED NATO NON CLASSIFIÉ ☐	PROTECTED A PROTÉGÉ A ☐
PROTECTED B PROTÉGÉ B ☐	NATO RESTRICTED NATO DIFFUSION RESTREINTE ☐	PROTECTED B PROTÉGÉ B ☐
PROTECTED C PROTÉGÉ C ☐	NATO CONFIDENTIAL NATO CONFIDENTIEL ☐	PROTECTED C PROTÉGÉ C ☐
CONFIDENTIAL CONFIDENTIEL ☐	NATO SECRET NATO SECRET ☐	CONFIDENTIAL CONFIDENTIEL ☐
SECRET SECRET ☐	COSMIC TOP SECRET COSMIC TRÈS SECRET ☐	SECRET SECRET ☐
TOP SECRET TRÈS SECRET ☐		TOP SECRET TRÈS SECRET ☐
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☐ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET– SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? ☑ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? ☑ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité UNCLASSIFIED

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	 B	 C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRES SECRET
Information / Assets Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
Security Classification / Classification de sécurité UNCLASSIFIED	

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Eric Poulin	Manager, Security Operations		
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613 991-5838		eric.poulin@canada.ca	25/11/2019

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Jean-Francois Houde	Manager, Security Services		
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613 949-6420			NOV 25 2019

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

☒ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
		Saumur, Jacques 0 Digitally signed by Saumur, Jacques 0 DN: c=CA, o=GC, ou=PWGSC-TPSGC, cn=Saumur, Jacques 0 Date: 2017.02.02 11:38:22 -05'00'	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**

Jacques Saumur
Contract Security Officer
Contracts Security Division|Division des contrats sécurité /
Contract Security Program|Programme de sécurité des contrats /
Public Services and Procurement Canada| Services publics et Approvisionnement Canada
Jacques.Saumur@tpsgc-pwgsc.gc.ca
Telephone | Téléphone 613-948-1732
Facsimile | Télécopieur 613-948-1712

ANNEXE G ENTENTE DE NON-DIVULGATION

Je soussigné(e), _____ , reconnais que, dans le cadre de mon travail à titre d'employé ou de sous-traitant de _____ , je peux avoir le droit d'accès à des renseignements fournis par ou pour le Canada relativement aux travaux, en vertu de la demande de soumission et contrat portant le numéro de série 0D160-204228, entre Sa Majesté la Reine du chef du Canada, représentée par le ministre des Travaux publics et des Services gouvernementaux et Sécurité publique Canada (SP), y compris des renseignements confidentiels ou des renseignements protégés par des droits de propriété intellectuelle appartenant à des tiers, ainsi que ceux qui sont conçus générés ou produits par l'entrepreneur pour l'exécution des travaux. Aux fins de cette entente, les renseignements comprennent, sans s'y limiter, tous les documents, instructions, directives, données, éléments matériels, avis ou autres, reçus verbalement, sous forme imprimée ou électronique ou autre, et considérés ou non comme exclusifs ou de nature délicate, qui sont divulgués à une personne ou dont une personne prend connaissance pendant l'exécution du contrat.

J'accepte de ne pas reproduire, copier, utiliser, divulguer, diffuser ou publier, en tout ou en partie, de quelque manière ou forme que ce soit les renseignements décrits ci-dessus sauf à une personne employée par le Canada qui est autorisée à y avoir accès. Je m'engage à protéger les renseignements et à prendre toutes les mesures nécessaires et appropriées, y compris celles énoncées dans toute instruction écrite ou orale, émise par le Canada, pour prévenir la divulgation ou l'accès à ces renseignements en contravention de cette entente.

Je reconnais également que les renseignements fournis à l'entrepreneur par ou pour le Canada ne doivent être utilisés qu'aux seules fins du contrat et ces renseignements demeurent la propriété du Canada ou d'un tiers, selon le cas.

J'accepte que l'obligation de cette entente survivra à la fin du contrat portant le numéro de série : 0D160-204228/001/HN

_____

Nom imprimé

_____

Titre

_____

Signature

_____

Date

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

Claim for Exchange Rate Adjustments
Demande de rajustement du taux de change

Contractor Name - Nom de l'entrepreneur	PWGSC File Number - Numéro du dossier de TPSGC	Contract Number - Numéro du contrat	Item/Invoice Number - Numéro d'article/de facture

1	2	3	4	5	6	7	8	9
Item Number Numéro d'article	Description	Foreign Currency Component (FCC) per Unit Montant en monnaie étrangère par unité **($CAN)**	Foreign Currency Devise étrangères	Quantity Quantité	Initial Exchange Rate Facteur de conversion initial **(i_0)**	Exchange Rate for Adjustments Taux de change aux fins du rajustement **(i_1)**	% Change Variation en % **$(i_1-i_0)/i_0 > 0.02$ (+/-)**	Adjustment = FCC X Quantity X **$(i_1 - i_0)/i_0$** Rajustement = montant en monnaie étrangère X Quantité X **$(i_1 - i_0)/i_0$**
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
								$ 0.000
					Total Exchange Rate Adjustment Rajustement total du taux de change			**$ 0.000**

Instructions

Where:

i_0 = initial exchange rate (CAN$ per unit of foreign currency [e.g. US$1])

i_1 = exchange rate for adjustment purposes (CAN$ per unit of foreign currency [e.g. US$1])

Instructions to bidders:

1. Bidders must complete columns (1) to (4) at time of bidding, for each line item where they want to invoke the exchange rate fluctuation provisions.

2. Where bids are evaluated in Canadian dollars, the dollar values provided in column (3) should also be in Canadian dollars, so that the adjustment amount is in the same currency as the payment.

Instructions for Payment:

1. This form must be submitted with the invoice for payment with respect to all items with an FCC. Complete columns (1) through (7). Columns (8) and (9) will auto complete.

2. Suppliers should submit a separate calculation sheet for each invoice submitted showing the exchange rate adjustment for all line items with an FCC.

3. This form must be provided with all invoices where the exchange rate fluctuates more than 2% (increase or decrease), (i.e. $abs[(i_1 - i_0) / i_0] > .02$), unless otherwise stated in the contract.

Étant entendu que :

i_0 = Facteur de conversion du taux de change initial ($ CA par unité de devise étrangère [p. ex. 1 $ US])

i_1 = Taux de change aux fins du rajustement ($ CA par unité de devise étrangère [p. ex. 1 $ US])

Instructions aux soumissionnaires :

1. Les soumissionnaires doivent remplir les colonnes (1) à (4) au moment de présenter leur soumission, pour chacun des produits pour lesquels ils veulent se prévaloir des dispositions relatives à la fluctuation du taux de change.

2. Lorsque les soumissions sont évaluées en dollars canadiens, les montants en dollars indiqués dans la colonne (3) doivent également être en dollars canadiens, de sorte que le montant du rajustement soit indiqué dans la même devise que pour le paiement.

Instructions relatives au paiement :

1. Le présent formulaire doit accompagner la facture en vue du paiement pour chaque article comportant un montant en monnaie étrangère. Il faut remplir les colonnes (1) à (7). Les colonnes (8) et (9) seront remplies automatiquement.

2. Les fournisseurs doivent présenter une feuille de calcul séparée pour chaque facture et indiquer le rajustement du taux de change pour chaque article comportant un montant en monnaie étrangère.

3. Le présent formulaire doit accompagner toutes les factures pour lesquelles la fluctuation du taux de change est supérieure à 2% (augmentation ou diminution), (c.-à-d. $abs[(i_1 - i_0) /i_0] > .02$), à moins d'indication contraire dans le contrat.