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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

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

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

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

Title - Sujet Transformation de la SSI - DP	
Solicitation No. - N° de l'invitation EP243-170549/B	**Amendment No. - N° modif.** 011
Client Reference No. - N° de référence du client 20170549	**Date** 2017-09-13
GETS Reference No. - N° de référence de SEAG PW-$$XE-678-31237	
File No. - N° de dossier 678xe.EP243-170549	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2017-10-02**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Oates, Christine	**Buyer Id - Id de l'acheteur** 678xe
Telephone No. - N° de téléphone (873) 469-3917 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

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

Canada

Modification nº 011

Objectif :

A. Relever les modifications à la demande de propositions (DP).
B. Répondre aux questions concernant la présente DP.
C. De déplacer la date de clôture au 2 octobre 2017.

A. MODIFICATIONS

Changement nº 91 :

Dans la section 1 de l'ANNEXE A : APERÇU DE LA SOLUTION DE SÉCURITÉ INDUSTRIELLE DU CANADA, 2.1 Nouvelle solution, **SUPPRIMER : Figure 1** : La carte interactive globale pour la solution de TSSI dans son intégralité et **REMPLACER** par la suivante :

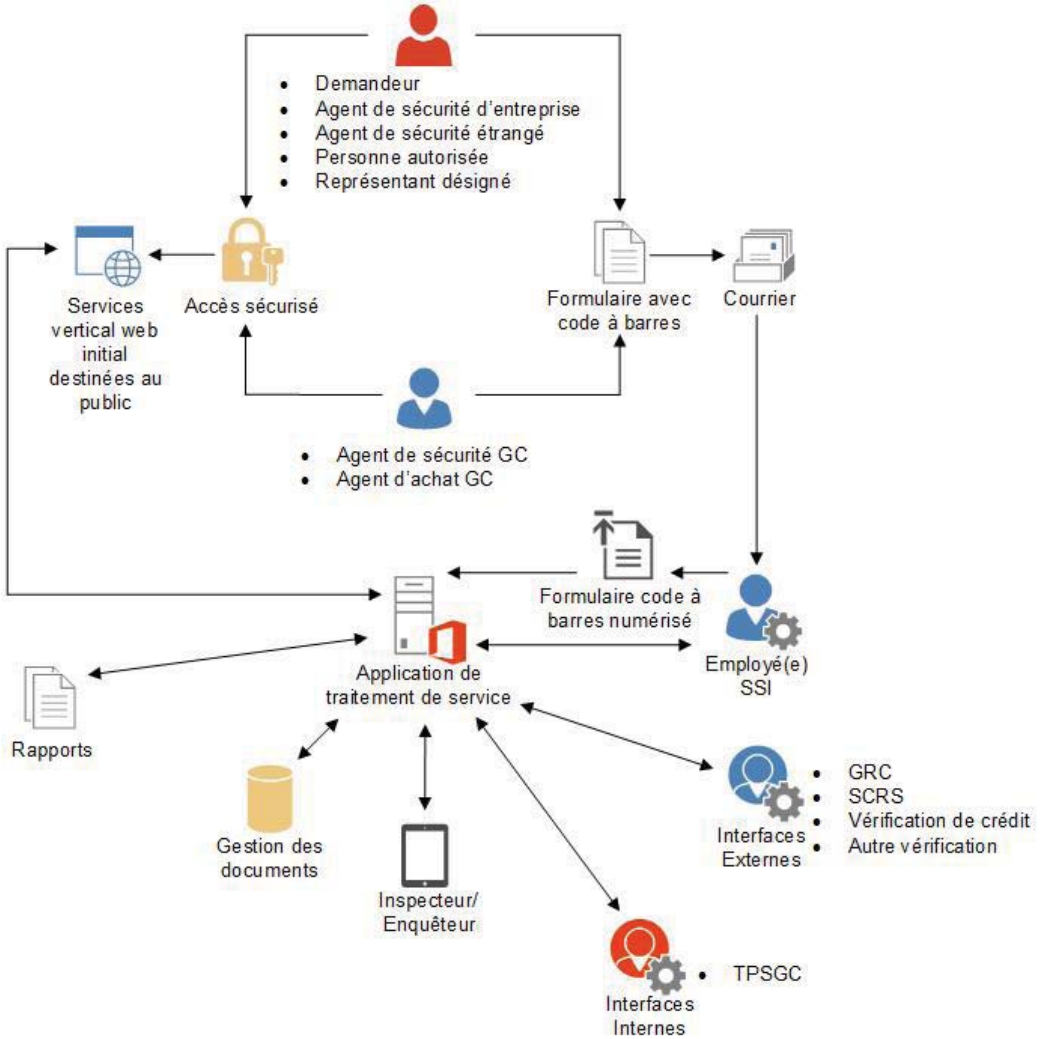


Figure 1 : Carte interactive globale pour la solution de TSSI.

SUPPRIMER :

Sont illustrés les types d'utilisateur principaux utilisant la technologie d'accès sécurisé du GC afin d'accéder au portail Web de la solution de TSSI afin de présenter des demandes de services à l'application de traitement des services de la solution de TSSI.

INSÉRER :

Sont illustrés les types d'utilisateurs principaux utilisant la technologie de services de cyberauthentification du GC pour accéder au service public Web vertical et frontal de la solution de TSSI afin de présenter des demandes de services à l'application de traitement des services de la solution de TSSI. Veuillez consulter le http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26262 pour plus d'informations à propos des services de cyberauthentification du GC.

Changement nº 92 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 1.2, Exigences détaillées — Restructuration des processus opérationnels :

INSÉRER :

EO nº 19	Préparer une stratégie préliminaire pour la restructuration des processus opérationnels, ce qui comprend notamment : (a) compréhension des processus opérationnels actuels du Secteur de la sécurité industrielle et la nécessité au recours de pratiques en matière de sécurité au sein des diverses opérations d'affaires; (b) plan pour effectuer une analyse des écarts dans le processus opérationnel; (c) compréhension des contraintes et des répercussions; (d) quatre exemples d'occasions d'accroître l'efficacité et la rentabilité des processus et les approches proposées en matière de mise en œuvre; (e) compréhension des risques et des options aux fins d'atténuation et de résolution des risques; (f) planification des activités de restructuration des processus opérationnels.
EO nº 20	Préparer une stratégie pour la restructuration des processus opérationnels après que la stratégie préliminaire pour la restructuration des processus opérationnels ait été évaluée par le Canada et jugée comme répondant aux bénéfices et aux exigences énoncés ci-dessus.

Changement nº 93 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.1, Sommaire des exigences — Exigences fonctionnelles :

SUPPRIMER :

La solution est une application opérationnelle qui comprend deux volets majeurs : une application de traitement des services et un portail Web.

INSÉRER :

La solution est une application opérationnelle qui comprend deux volets majeurs : une application de traitement des services et un service public Web vertical et frontal.

SUPPRIMER :

Le portail Web est le volet d'échange de données sur Internet de la solution qui est utilisé par le public et qui sert d'interface libre-service centrale et habilitante permettant les communications et les interactions entre les utilisateurs externes et les deux programmes du Secteur de la sécurité industrielle : le Programme de sécurité des contrats et le Programme des marchandises contrôlées. L'entrepreneur doit fournir une solution avec un portail Web qui :

INSÉRER :

Le service public Web vertical et frontal est le volet d'échange de données sur Internet de la solution qui est utilisé par le public et qui sert d'interface libre-service centrale et habilitante permettant les communications et les interactions entre les utilisateurs externes et les deux programmes du Secteur de la sécurité industrielle : le Programme de sécurité des contrats et le Programme des marchandises contrôlées. L'entrepreneur doit proposer une solution avec un service public Web vertical et frontal qui :

Changement nº 94 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-AU.02, point D, dans son intégralité et **REMPLACER** par ce qui suit :

d) Disponibilité du certificat d'approbation approprié destiné aux utilisateurs externes aux fins de téléchargement/impression à partir du service public Web vertical et frontal.

Changement nº 95 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2,2.1 - Application de traitement des services, **SUPPRIMER** APP-AU.04 dans son intégralité et **REMPLACER** par ce qui suit :

APP-AU.04	Chargement automatique d'un calendrier sur le service public Web vertical et frontal qui avisera l'utilisateur externe d'événements prédéterminés liés à des demandes de services aux SSI (p. ex., les dates d'échéance de correspondance et les renouvellements d'inscription des organisations).

Changement nº 96 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-OPS.07 dans son intégralité et **REMPLACER** par ce qui suit :

APP-OPS.07	Permet aux utilisateurs internes disposant des autorisations appropriées de faire preuve de souplesse et d'adaptabilité afin de mettre en œuvre ultérieurement des politiques, processus et règles administratives et de modifier ceux déjà utilisés par la solution dans son ensemble, c.-à-d. par le service public Web vertical et frontal et par l'application de traitement interne. Par exemple, ces utilisateurs doivent être en mesure de modifier le paramètre de la solution définissant la norme relative au nombre de jours pour remplir une demande d'inscription au PMC. La modification est alors automatiquement reportée dans tous les rapports et tableaux de bord, et utilisée dans tous les calculs internes.

Changement nº 97 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-OPS.10 dans son intégralité et **REMPLACER** par ce qui suit :

APP-OPS.10	Permet aux utilisateurs internes disposant des autorisations nécessaires de modifier les formulaires externes et de les publier au service public Web vertical et frontal.

Changement nº 98 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-OPS.19 dans son intégralité et **REMPLACER** par ce qui suit :

APP-OPS.19	Permet aux utilisateurs internes disposant des autorisations appropriées de pouvoir faire une copie d'une demande de service en lecture seule en cours afin de faciliter le traitement des demandes de renseignements et d'inscription. La demande de service copiée devrait afficher les mêmes éléments que celle que l'utilisateur externe consulte sur le service public Web vertical et frontal. Cela permet à l'utilisateur interne de voir ce que l'utilisateur externe voit à l'écran et vice versa.

Changement nº 99 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-OPS.22 dans son intégralité et **REMPLACER** par ce qui suit :

APP-OPS.22	Permet aux utilisateurs internes disposant des autorisations nécessaires d'ouvrir et de fermer l'accès à un lien pouvant être utilisé par les utilisateurs pour accéder au service public Web vertical et frontal afin d'avoir accès à l'environnement de mise à l'essai/formation. Voir l'exigence opérationnelle WP-EU 22.

Changement nº 100 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-COM.06 dans son intégralité et **REMPLACER** par ce qui suit :

APP-COM.06	Permet aux utilisateurs internes de produire et d'imprimer la correspondance à envoyer par les services postaux (p. ex., la transmission d'un code d'autorisation lors d'une authentification initiale dans le service public Web vertical et frontal aux personnes autorisées à la Direction des marchandises contrôlées).

Changement nº 101 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-PPL.03 dans son intégralité et **REMPLACER** par ce qui suit :

APP-PPL.03	Permet aux utilisateurs internes de soumettre des renseignements concernant les demandes de services dans l'application de traitement des services de la solution par le balayage numérique du code à barres généré par le formulaire (pour compléter les fonctionnalités du service public Web vertical et frontal relatives aux demandes de services soumises par d'autres voies de communication [le courriel, par exemple]; de plus, cela élimine la nécessité d'entrer manuellement les données recueillies dans les formulaires de demande de services déposés).

Changement nº 102 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-ICN.04 dans son intégralité et **REMPLACER** par ce qui suit :

APP-ICN.04	Accéder aux résultats de vérification de casier judiciaire et d'empreintes digitales de la GRC, afin d'établir une correspondance entre une demande de services soumise, les empreintes digitales correspondantes et les résultats obtenus. L'établissement de la correspondance se fait au moyen d'un numéro de contrôle de document unique fourni au demandeur par la GRC; ce numéro doit être fourni dans le cadre des renseignements soumis avec la demande de services. Ce processus doit être automatiquement enclenché lorsqu'une demande de services est soumise avec succès dans l'application de traitement à partir du service public Web vertical et frontal. Il doit également être disponible sous forme d'option activée sur demande par des utilisateurs internes.

Changement nº 103 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-RP.12 dans son intégralité et **REMPLACER** par ce qui suit :

APP-RP.12	Permet aux utilisateurs internes de promouvoir un rapport ou de le rétrograder d'un statut de traitement des demandes à un statut de rapport standard, leur permettant alors d'être inclus dans l'ensemble de rapports standard de la solution, tant à l'externe (service public Web vertical et frontal) qu'à l'interne (traitement des demandes).

Changement nº 104 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.1 - Application de traitement des services, **SUPPRIMER** APP-RP.14 dans son intégralité et **REMPLACER** par ce qui suit :

APP-RP.14	Permet aux utilisateurs internes de modifier les critères de sélection associés à des rapports normalisés mis à la disposition des utilisateurs externes sur le service public Web vertical et frontal.

Changement nº 105 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, **SUPPRIMER** l'en-tête de 2.2.2 - Portail Web et **REMPLACER** par l'en-tête 2.2.2 - Service public Web vertical et frontal.

Changement nº 106 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.2, Service public Web vertical et frontal :

SUPPRIMER :

L'entrepreneur doit livrer un portail Web qui comporte, sans s'y limiter, les fonctionnalités suivantes :

INSÉRER :

L'entrepreneur doit livrer un service public Web vertical et frontal qui comporte, sans s'y limiter, les fonctionnalités suivantes :

Changement nº 107 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.2, Service public Web vertical et frontal, **SUPPRIMER** WP-SH.05 dans son intégralité et **REMPLACER** par ce qui suit :

WP-SH.05	Permet un échange synchronisé d'information entre le service public Web vertical et frontal et l'application de traitement des services.

Changement nº 108 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.2, Service public Web vertical et frontal, **SUPPRIMER** WP-UE.05 dans son intégralité et **REMPLACER** par ce qui suit :

WP-UE.05	Permet aux utilisateurs externes d'employer des appareils mobiles dotés de fureteurs Internet pour accéder au service public Web vertical et frontal en tout temps. Comprend la signature électronique.

Changement nº 109 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.2, Service public Web vertical et frontal, **SUPPRIMER** WP-UE.06 dans son intégralité et **REMPLACER** par ce qui suit :

WP-UE.06	Permet aux utilisateurs externes d'accéder au service public Web vertical et frontal à partir de tablettes dotées de fureteurs Internet sans perdre aucune des fonctionnalités du service public Web vertical et frontal.

Changement nº 110 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.2, Service public Web vertical et frontal, **SUPPRIMER** WP-UE.17 dans son intégralité et **REMPLACER** par ce qui suit :

WP-UE.17	Permet aux utilisateurs externes de naviguer dans le service public Web vertical et frontal d'une manière conforme aux normes pour le Web du GC.

Changement nº 111 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.2, Service public Web vertical et frontal, **SUPPRIMER** WP-UE.22 dans son intégralité et **REMPLACER** par ce qui suit :

WP-UE.22	Environnement de formation de l'utilisateur externe : permet aux utilisateurs externes d'accéder à un environnement public de formation distinct ou à un environnement de mise à l'essai leur permettant de découvrir les services fournis par le SSI et d'apprendre à les utiliser. Cet environnement de formation ne doit afficher que les fonctionnalités du service public Web vertical et frontal et ne doit pas conserver ni ne transmettre de données.

Changement nº 112 :

Dans la SECTION 2 DE L'ANNEXE A, EXIGENCES OPÉRATIONNELLES, 2.2.3 - Migration des données, **SUPPRIMER** APP-DM.04 dans son intégralité et **REMPLACER** par ce qui suit :

APP-DM.04	Aider le gouvernement du Canada en matière d'orientation et de documentation pour la migration de l'échantillon de données et la validation des données. Évaluer l'intégrité des données et l'incidence de la migration vers le nouveau système. L'échantillon de données doit comprendre 50 enregistrements de chaque processus, p.ex., une attestation de sécurité du personnel, les marchandises contrôlées, etc. Faire rapport des constatations au responsable du projet en indiquant le degré de réussite de l'approche de migration.

Changement nº 113 :

SUPPRIMER la SECTION 3 DE L'ANNEXE A, EXIGENCES TECHNIQUES dans son intégralité et **REMPLACER** par ce qui suit :

PARTIE 3 : EXIGENCES TECHNIQUES

Cette section définit les exigences techniques pour la solution.

1.1 APERÇU DES EXIGENCES

L'entrepreneur doit concevoir, élaborer, configurer, mettre à l'essai, mettre en œuvre, déployer et stabiliser une solution fondée sur des exigences précises, l'architecture conceptuelle de la solution ISST de haut niveau et l'utilisation des technologies énumérées dans cet énoncé des travaux. La solution doit être conviviale, fiable, adaptable, extensible, interopérable et extensible de manière à pouvoir être ajustée en fonction des processus opérationnels ayant fait l'objet de modifications, d'adaptations ou d'ajouts ainsi que des fonctions automatisées du système. La solution doit également être conforme aux politiques, aux lignes directrices et à l'environnement du GC en matière de TI-GI.

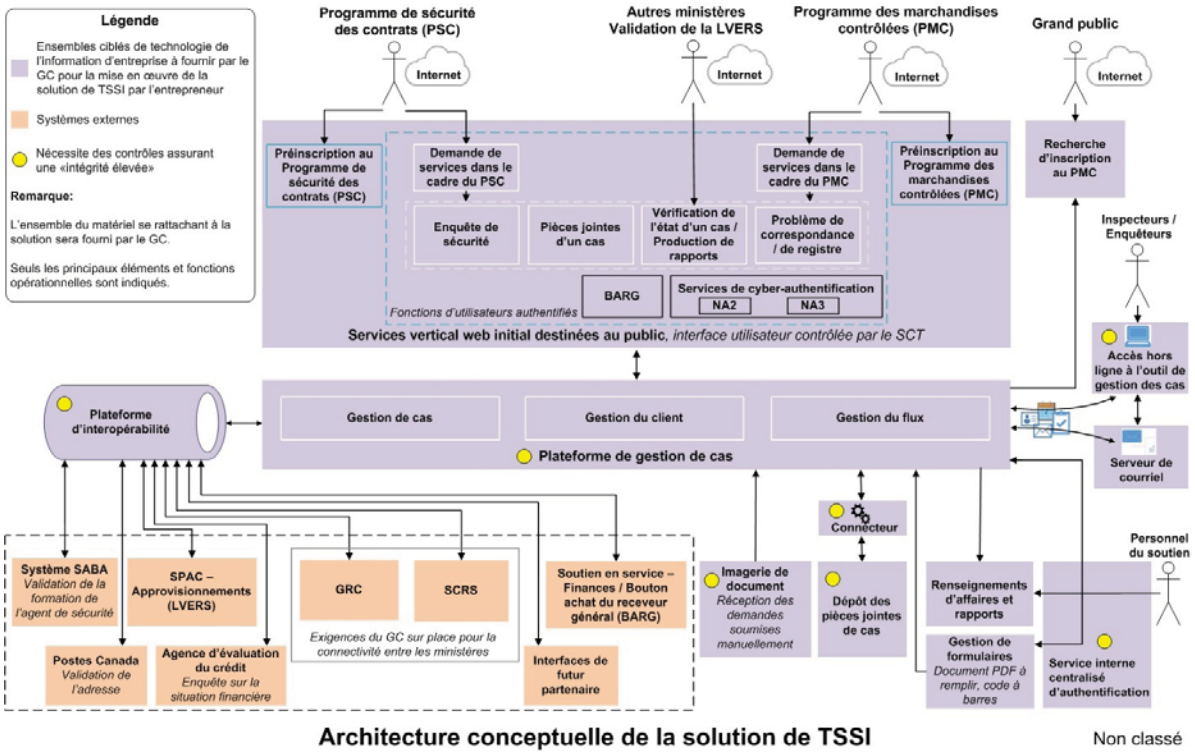


Figure 2: Diagramme d'architecture de la solution ISST de haut niveau.

Microsoft Dynamics CRM est la principale plateforme de la solution du SSI offrant des capacités comme la gestion des cas et des clients, de même que des flux de travaux à des fins d'automatisation des processus opérationnels. L'accès à cette plateforme devra être accordé au personnel de soutien du SSI une fois qu'il aura été authentifié au moyen du service d'authentification d'accès sécurisé. Les inspecteurs sur le terrain pourront aussi interagir avec la plateforme principale MS Dynamics CRM à l'aide de capacités d'accès hors ligne reposant sur Microsoft Dynamics CRM pour Outlook.

Les utilisateurs externes, par exemple les demandeurs du Programme de la sécurité des contrats et du Programme des marchandises contrôlées, auront accès à la fonctionnalité requise pour leurs processus opérationnels par l'intermédiaire des services Web de première ligne, verticaux et accessibles au public. Ces utilisateurs auront accès à l'environnement après avoir été authentifiés selon le niveau d'assurance approprié requis par l'application à l'aide des services d'authentification électronique et en fonction de rôles et de droits bien précis. **Aucun** accès direct à la plateforme principale MS Dynamics CRM ne sera accordé aux utilisateurs externes. La plateforme des services Web de première ligne, verticaux et accessibles au public permettra d'héberger des formulaires Web conçus pour la demande et la réception des services. La configuration des services Web de première ligne, verticaux, accessibles au public et habilitant les interfaces des processus opérationnels liés à la réception des demandes doit satisfaire aux exigences du GC (WCAG) en matière de normes Web.

L'entrepreneur devra configurer la technologie qui résidera sur le réseau du GC, ainsi que l'interface avec la plateforme de gestion des cas Dynamics CRM. La solution devra être extensible de manière à répondre

aux besoins du développement futur, reposer sur les services Web et privilégier principalement la configuration par rapport à la personnalisation.

L'accès des utilisateurs aux différentes fonctionnalités de l'application sera accordé au moyen des privilèges et des configurations d'accès fondés sur le rôle des plateformes technologiques sous-jacentes en fonction des profils d'accès des utilisateurs.

La solution doit tirer parti de la technologie décrite par TPSGC dans la liste descriptive ci-dessous. Ces technologies sont des suites cibles de TI d'entreprise qui sont dictées par les directions du dirigeant principal de l'information (DDPI) du SCT ou de TPSGC, afin de réduire et de rationaliser l'empreinte des applications du GC et de TPSGC. Dans la mesure du possible, l'entrepreneur doit satisfaire aux exigences de la solution, ainsi qu'à toutes les nouvelles exigences découlant de la restructuration des processus opérationnels en mettant à profit ces technologies de manière à développer une solution unifiée.

Les suites cibles de TI d'entreprise mentionnées auxquelles l'entrepreneur doit se conformer comprennent, entre autres, les suivantes :

(a) **Dynamics CRM (sur place) 2015 (ou version ultérieure) (suite cible de TI d'entreprise) Technologie de gestion des cas** – Les services Web de première ligne, verticaux et accessibles au public pour la réception des demandes des entreprises permettront d'échanger des informations avec un outil de gestion des relations avec la clientèle, MS Dynamics CRM (sur place) 2015 (ou version ultérieure), afin d'entreprendre, de gérer et d'exécuter des activités de gestion de cas et d'échanger des informations à ce sujet. L'outil de gestion des cas est un service géré de façon centralisée et sera utilisé par les utilisateurs internes ayant des rôles et des droits bien définis.

(b) **Microsoft Exchange Server, Client d'Outlook (suite cible de TI d'entreprise) et MS Dynamics CRM pour le courriel Outlook du GC** – Cette technologie servira à soutenir les capacités de courriel et de gestion des cas hors ligne pour les utilisateurs internes, comme les inspecteurs sur le terrain.

(c) **Business Objects de SAP (suite cible de TI d'entreprise) Établissement de rapports relatifs aux renseignements d'affaires** – La suite Business Objects BI de SAP permet aux entreprises de réaliser des analyses opérationnelles. En ce qui concerne cette solution, toutefois, les fonctionnalités comprenant des tableaux de bord destinés aux utilisateurs internes mettront d'abord à profit les capacités d'établissement de rapports qu'offrent les outils de Dynamics CRM 2015 (ou une version ultérieure). Si ces derniers ne permettent pas d'établir des rapports stratégiques, la suite Business Objects BI de SAP, reliée à un entrepôt de données pures, effectuera cette tâche. Les fonctions de production de rapports doivent être mises à la disposition des utilisateurs internes et externes selon les profils d'accès des utilisateurs.

(d) **Service Bus d'Oracle (suite cible de TI d'entreprise) Technologie de partage de l'information** – Plateforme d'interopérabilité du GC (PIGC – basée sur Service Bus d'Oracle (technologie). Le partage de l'information entre le Secteur de la sécurité industrielle (SSI) et les organisations

partenaires doit être automatisé et géré selon les capacités de la PIGC et de la technologie sous-jacente de Service Bus d'Oracle.

(e) Système d'imagerie et de numérisation – Ce système est en place et utilise la technologie DataCap d'IBM. La solution de l'ISST devra permettre l'échange de l'information avec ce système.

(f) Système de gestion des documents et des dossiers – La solution devrait nécessiter l'entreposage, la gestion et l'extraction des données regroupées principalement en deux catégories : (1) Système de gestion des bases de données ou des données – Données structurées faisant l'objet d'un grand nombre d'opérations de traitement et de transactions, habituellement associées aux demandes en cours de traitement et aux données sur les entreprises et le personnel; et (2) Système de gestion des documents et des dossiers – Données non structurées habituellement associées à des pièces jointes qui ne doivent pas être modifiées, mais qui doivent être conservées à des fins de gestion des documents et des dossiers et à des fins de preuve (p. ex., passeports, certificats de naissance, etc.), ce qui représente un volume inférieur de transactions ainsi qu'un faible taux d'extraction de données.

i) **Système de gestion des bases de données ou des données** – L'entrepreneur doit tirer parti des produits existants déjà autorisés et utilisés par SPAC, afin de satisfaire aux exigences liées au traitement de l'information et des données non sensibles, sensibles et intensives. La solution doit respecter les normes de SQL Server ou d'Oracle du GC pour toutes les applications de bases de données.

ii) **Système de gestion des documents et des dossiers** – La norme actuelle du GC pour la gestion des documents et des dossiers est Content Server d'OpenText, qui devrait être utilisée pour l'entreposage à long terme des données non structurées. Il s'agit de la valeur par défaut pour les éléments qui ne sont pas nécessaires au traitement dynamique, tels que (sans toutefois s'y limiter) les pièces jointes statiques et les formulaires soumis en personne qui sont numérisés à des fins de gestion des documents et des dossiers.

L'entrepreneur doit assurer une expertise technique en matière de GI-TI dans les domaines relatifs au développement des applications, notamment en ce qui touche le langage de programmation C# et Java, la configuration et l'intégration, la restructuration des processus opérationnels, l'intégration de l'information, ainsi que la sécurité des applications et des données.

L'ensemble du matériel se rattachant à la solution sera fourni par le GC et aucune autre installation matérielle (outre celles que requiert la connectivité au réseau) ne sera nécessaire. Si l'entrepreneur utilise des outils logiciels ne se trouvant pas dans le GC, il lui faut faire approuver ces outils par le GC avant de commencer le processus d'installation pour TPSGC. L'entrepreneur doit travailler en étroite collaboration avec Services partagés Canada (SPC) pour faire en sorte que les capacités matérielles respectent ou surpassent les exigences de la solution globale.

1.2 EXIGENCES TECHNIQUES

L'entrepreneur doit mettre en œuvre une solution qui réponde, sans pour autant s'y limiter, aux exigences énumérées ci-dessous.

Section de l'EDT	Exigence
Tech.01	Mettre en œuvre les pages Web dont le codage est UTF-8.
Tech.02	Mettre en œuvre l'intégration en temps réel au moyen d'une architecture de services Web telle que REST (HTTP, codage JSON ou XML) et SOAP (HTTP ou JMS).
Tech.03	Permettre aux utilisateurs externes d'exporter les résultats, notamment des rapports et des résultats de recherche, sous forme de tableau ou de graphique, dans tous les formats qui satisfont spécifiquement aux exigences des WCAG 2.0 et assurer la mise en œuvre du processus d'exportation.
Tech.04	Respecter les pratiques exemplaires de sécurisation des services Web, comme celles du guide sur les services Web sécurisés (publication spéciale 800-95 du National Institute of Standards and Technology [NIST]) et de la deuxième version des directives sur la sécurisation des serveurs Web publics (publication spéciale 800-44 du NIST).
Tech.05	Permettre la fermeture automatique d'une session Web ouverte après un délai d'inactivité qui sera fixé par le GC et assurer la mise en œuvre du processus de fermeture.
Tech.06	Permettre aux utilisateurs internes d'exporter les résultats, notamment des rapports et des résultats de recherche, sous forme de tableau ou de graphique, dans les formats de fichier suivants qui satisfont aux techniques énoncées dans les WCAG 2.0 (https://www.canada.ca/fr/secretariat-conseil-tresor/services/communications-gouvernementales/boite-outils-experience-web.html) en ce qui a trait aux essais de conformité : (a) PDF (PDF d'Adobe); (b) DOC, DOCX (MS Word 2013 et version ultérieure); (c) XLS, XLSX (MS Excel 2013 et version ultérieure).
Tech.07	Mettre en œuvre la solution afin de prendre en charge la norme la plus récente du GC en matière de navigateur Web (à l'heure actuelle, Microsoft Internet Explorer 11), ainsi que deux versions précédentes d'importance du navigateur Microsoft à mesure qu'évoluent les normes.
Tech.08	Mettre en œuvre une solution compatible avec les principaux navigateurs Web qui prennent en charge le protocole de chiffrement TLS 1.2 offert sur le marché à l'heure actuelle (tels Firefox, Safari et Chrome, pour ne nommer que ceux-là). Consulter le glossaire (Appendice 5 de l'Annexe A) afin d'obtenir plus de renseignements.

Section de l'EDT	Exigence
Tech.09	Proposer une solution sécurisée axée sur un navigateur Web dont l'installation sur le poste de travail de l'utilisateur interne ne requiert aucun autre logiciel de bureau que le navigateur Web, « Microsoft Dynamics CRM for Outlook » afin d'assurer la gestion des cas hors ligne, et MS Outlook.
Tech.10	Mettre en œuvre l'acceptation et le téléchargement de documents d'appui et de pièces jointes dont la taille maximale pourrait excéder 30 mégaoctets, ainsi que de tous les formats de fichiers.
Tech.11	Mettre en œuvre la validation et la confirmation de la saisie des données selon le type de champ, la taille des données, les propriétés du tableau et la liste des valeurs préconfigurées (p. ex., pour le code postal, seul le format valide sera accepté).
Tech.12	Utiliser les services Web de première ligne, verticaux et accessibles au public pour faciliter les processus de réception des demandes des entreprises, comme la création de formulaires Web pour recueillir et échanger de l'information, et qui sont intégrés aux entités MS Dynamics CRM 2015 (ou version ultérieure) et qui prennent en charge les techniques Tech14 et Tech.18.
Tech.13	Offrir un style d'architecture permettant une bonne gestion des erreurs, la restauration et la notification aux utilisateurs lorsque des erreurs se produisent en ligne.
Tech.14	Par souci de convivialité, intégrer les pratiques exemplaires quant aux principes de conception des applications Web (en d'autres termes, mettre à profit les meilleures pratiques en matière d'applications Web [W3] : boutons d'activation et de désactivation, options et transmission des données fondées sur les valeurs saisies par l'utilisateur, réduction des messages-guides inutiles, etc.).
Tech.15	Utiliser au maximum la fonction intégrée d'établissement de rapports de l'application MS Dynamics CRM 2015 (ou d'une version ultérieure) pour permettre à la communauté des utilisateurs internes d'établir des rapports opérationnels et de se servir du tableau de bord et, dans la mesure du possible, de préparer des rapports stratégiques.
Tech.16	Tirer parti de la capacité de la plateforme de renseignements d'affaires du GC pour mettre en œuvre des fonctions d'établissement de rapports que n'offre pas la solution axée sur MS Dynamics CRM (sur place) 2015 (ou une version ultérieure). L'entrepreneur devra pour ce faire créer des scripts d'extraction, de transformation et de chargement (ETC) qui copieront automatiquement les données de la base de données de la solution pour les intégrer à la plateforme de renseignements d'affaires du GC et doter ainsi cette dernière de fonctions relatives à l'établissement de rapports et au tableau de bord. L'entrepreneur développera ces fonctions de telle sorte qu'elles puissent soutenir les décisions opérationnelles.

Section de l'EDT	Exigence
Tech.17	Satisfaire aux exigences pertinentes du profil de sécurité « Protégé B, Intégrité élevée, disponibilité moyenne » (PB/É/M) pour les plateformes indiquées dans le diagramme de l'architecture conceptuelle de l'ISST.
Tech.18	Assurer la conformité aux normes Web du GC (https://recherche-search.gc.ca/rGs/s_r?cdn=canada&st=s&num=10&langs=en&st1rt=1&s5bm3ts21rch=x&q=web+standards&_charset_=utf-8&wb-srch-sub=) et aux normes sur l'accessibilité des sites Web (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601) pour les processus de réception des demandes des entreprises reposant sur les services Web de première ligne, verticaux et accessibles au public.
Tech.19	Favoriser l'extensibilité, si une extension de la communauté d'utilisateurs ou une fonctionnalité de la solution est nécessaire pour soutenir les initiatives du GC.
Tech.20	Fournir une réponse sous la forme d'un accusé de réception ou d'un numéro de cas à un utilisateur externe dans un délai acceptable (en temps quasi réel) après la réception d'une demande unique correctement remplie (le GC déterminera le délai de réponse acceptable).
Tech.21	Créer et transmettre des renseignements aux utilisateurs au moyen d'avis.
Tech.22	Appuyer le concept d'architecture ouverte et donner l'accès à ses services et à ses fonctions au moyen d'API, de services Web et de technologies similaires.
Tech.23	Au cours de la période de transition, favoriser l'échange de données à partir des systèmes en place et vers ceux-ci par les moyens suivants : (a) temps quasi réel ou lots; (b) services Web ou API; (c) langage XML ou fichier non hiérarchique; (d) exportation et importation des données et du contenu; (e) messagerie d'entreprise ou ESB.
Tech.24	Recourir aux Services gérés de transfert sécurisé de fichiers (SGTSF) pour faire passer les fichiers numérisés dans le Système partagé de gestion des cas (SPGC).
Tech.25	Favoriser l'intégration par l'insertion de formulaires PDF intelligents ou à codes à barres auxquels l'utilisateur accède manuellement, ou à l'aide d'autres outils de numérisation afin de faciliter le traitement des cas sur support papier.

Section de l'EDT	Exigence
Tech.26	Tirer parti et soutenir des normes et des pratiques exemplaires de l'industrie des technologies de l'information et du GC qui ont été adoptées à grande échelle pour la création et le maintien d'un système informatique performant afin de répondre aux besoins suivants : (a) Fournir des applications Web conviviales; (b) Assurer et maximiser la maintenabilité de la solution; (c) Assurer et atteindre un niveau de fiabilité élevé; (d) Assurer l'extensibilité et la viabilité; (e) Garantir un niveau de performance acceptable du système
Tech.27	Soutenir les plans stratégiques du GC au chapitre de l'interopérabilité des applications, y compris, à tout le moins, par les moyens suivants : (a) en présentant ses fonctionnalités par l'intermédiaire d'une API qui tire parti des protocoles d'API conformes aux normes de l'industrie (ces fonctionnalités comprennent la capacité d'afficher au besoin les processus opérationnels contenus dans la solution); (b) en respectant les normes du GC – la Plateforme d'interopérabilité du GC (PIGC) qui sera normalisée selon la technologie de service Oracle Bus.
Tech.28	Interagir avec les éléments de technologie de l'information du GC (p. ex., l'infrastructure et la plateforme) sans qu'il soit nécessaire de transformer l'infrastructure existante du GC ou de modifier les postes de travail. Voici une liste des types de technologies qui devraient être pris en charge : (a) SAML 2.0 (b) JSON (c) Kerberos (d) X.509 (e) LDAP (f) CAFR (contrôle d'accès fondé sur les rôles) (g) OAuth (h) SOAP (i) REST (j) OData

Section de l'EDT	Exigence
Tech.29	Prendre en charge, utiliser ou développer des interfaces externes structurées et modulaires qui permettront l'échange de renseignements entre la solution et les autres systèmes par l'intermédiaire d'une infrastructure de communication sécurisée. Ces interfaces comprennent à tout le moins : a) Un intranet ou un extranet pour les processus opérationnels décrits dans la partie 2, « Exigences opérationnelles »; b) Des services Web – source de données de tiers; c) Des composantes de sécurité de tiers offertes sur le marché, par exemple des produits d'infrastructure à clés publiques (ICP); d) Des systèmes du GC ou des organisations non gouvernementales contenant les renseignements à l'appui nécessaires au traitement des transactions.
Tech.30	Interagir avec d'autres systèmes et plateformes comme l'indique le diagramme qui précède, en utilisant à tout le moins les éléments suivants : (a) API; (b) exportation et importation des données et du contenu; (c) messages utilisant le protocole Simple Object Access (SOAP) ou échanges de fichiers au moyen de l'Enterprise Service Bus [ESB] d'Oracle.
Tech.31	Inclure la protection des données transactionnelles en transit et statiques par le recours au Centre de la sécurité des télécommunications Canada (CSTC), à des algorithmes de chiffrement approuvés par le SCT ou par d'autres moyens que le GC estime acceptables.

L'entrepreneur doit :

Section de l'EDT	Exigence
Tech.32	Établir et soutenir, pour la durée du contrat et suivant les besoins, des environnements de simulation distincts au niveau de l'application aux fins de configuration, de mise à l'essai, de déploiement ainsi que de formation relativement aux nouvelles versions de la solution. Après le lancement de la solution, ces environnements demeureront en tout ou en partie et seront utilisés pour les activités en cours : l'entrepreneur devra donc assurer le transfert sans heurt des environnements configurés au GC.
Tech.33	Concevoir, développer, configurer, mettre à l'essai et prendre en charge la base de données de la solution afin de stocker, de gérer et de protéger les données allant jusqu'au niveau Protégé B.
Tech. 34	Élaborer des plans d'architecture logique et physique de l'ISST (à l'aide de modèles GC) en fonction du modèle d'architecture conceptuelle ISST. Ces plans sont soumis à l'approbation du GC.

Section de l'EDT	Exigence
Tech.35	Transférer au personnel de TPSGC les connaissances techniques liées au système et veiller à remettre au Ministère des copies de toute la documentation qui s'y rattache, y compris, mais sans s'y limiter, les documents portant sur la sécurité, la configuration fonctionnelle et non fonctionnelle, les livrets de conception et les dossiers d'exploitation et cela, avant l'achèvement des travaux.
Tech.36	Concevoir et créer une architecture de données présentant les caractéristiques suivantes : (a) inclut tous les modèles de données conceptuels, logiques et physiques pertinents; (b) définit, en collaboration avec TPSGC, les politiques, les règles et les normes liées à la gouvernance des données, notamment la façon dont celles-ci seront stockées, organisées, intégrées et mises à profit dans le cadre de la solution; (c) inclut des dictionnaires de données; (d) fonctionne dans l'environnement de la solution du SSI; (e) soutient l'ensemble des processus opérationnels du SSI; (f) soutient les exigences en matière de sécurité décrites dans le présent document (consulter la partie 5, qui porte sur les exigences relatives à la sécurité de la TI).
Tech.37	En collaboration avec le GC, effectuer la mise en correspondance des données des systèmes en place et de celles de la solution, et procéder à l'analyse des écarts.
Tech.38	Développer la documentation d'interface détaillée, incluant, mais sans s'y limiter: (a) Concept des opérations; (b) Vue d'ensemble des systèmes; (c) Vue d'ensemble de l'interface (pour chaque Interface dans, vers et de l'application); (d) Allocation fonctionnelle; (e) Transfert de données; (f) Transactions; (g) Sécurité et intégrité; (h) Exigences relatives à l'interface; (i) Exigences relatives au temps de traitement de l'interface; (j) Exigences relatives aux messages (ou fichiers); (k) Méthodes de communication; (l) Exigences de sécurité; (m) Méthodes de qualification; (n) Approbations; (o) Registre des changements.
Tech.39	Permettre la gestion des formulaires au moyen de la configuration dans *Dynamics* (ou un autre moyen) sans avoir besoin d'un développeur.
Tech.40	Acheter et configurer une technologie commerciale de portail Web qui satisfait aux exigences de la demande de soumissions actuelle.
Tech.41	Installer et exécuter sur *Windows Server 2012* et le serveur Web Internet Information Services (IIS).
Tech.42	Exploiter majoritairement; configuration par rapport à personnalisation.

Section de l'EDT	Exigence
Tech.43	Se rattacher au réseau du GC et être échelonnable.
Tech.44	Être configurable pour permettre l'intégration des justificatifs de la Fédération des justificatifs du gouvernement du Canada (FJGC).
Tech.45	Interface/intégration uniforme avec *MS Dynamics CRM* (2015 ou version plus récente) au moyen de services Web et/ou d'autres méthodes approuvées et soutenues par les plateformes de technologie sous-jacentes pour son intégration à la plateforme de gestion des cas *Dynamics CRM*.
Tech.46	Permettre la création et la publication de contenu dans les deux langues officielles du Canada, soit le français et l'anglais.
Tech.47	Configurer une solution qui répond aux exigences de la demande de soumissions en cours.
Tech.47A	Fournir des spécifications de conception détaillées.
Tech.47B	Fournir une approche relative à la gestion des relations, incluant les éléments suivants : a) Approche globale relative à la gestion des relations entre le gouvernement et l'entrepreneur; b) Communications entre le gouvernement du Canada et l'entrepreneur en ce qui a trait au un modèle de gouvernance et à la structure de l'équipe proposés, comme défini au point A du C1; c) Gestion et résolution de problèmes; d) Planification mixte et gestion des changements à la portée et au calendrier du projet

L'entrepreneur doit utiliser un service de front-end pour la technologie d'admission d'entreprise qui:

Tech.48	Permettre le chiffrement.
Tech.49	L'entrepreneur doit concevoir la solution pour veiller à ce que des « signatures numériques » soient utilisées à la fois pour les processus entamés par un utilisateur interne et par un service interne, au besoin.
Tech.50	L'entrepreneur doit déterminer et décrire, en tenant compte de la conception de son architecture physique, les contrôles de sécurité qui doivent être mis en œuvre par l'entrepreneur et le GC.
Tech.51	L'entrepreneur doit définir le contenu de la solution et configurer celle-ci afin de produire des dossiers de vérification générés par le système qui comprendront de l'information pour faciliter la détermination des infractions à l'intégrité.
Tech.52	Assurer l'échange de l'information et une intégration avec MS Dynamics CRM (2015 ou version ultérieure) à l'aide des services Web ou d'autres méthodes approuvées et prises en charge par les plateformes technologiques sous-jacentes pour assurer l'intégration de la solution avec la plateforme de gestion des cas de Dynamics CRM.
Tech.53	L'entrepreneur doit créer un processus qui permettra d'enregistrer les configurations antérieures de la solution pour appuyer le retour à une version antérieure pour une période qui sera définie par le GC.

Tech.54	L'entrepreneur doit configurer la solution pour prévenir le transfert d'information non autorisé et involontaire au moyen de ressources système partagées.
Tech.55	L'entrepreneur doit configurer la solution pour répondre automatiquement lorsque des infractions à l'intégrité se produisent.

Changement nº 114 :

Dans la SECTION 4 DE L'ANNEXE A, ACCÈS SÉCURISÉ, 1.2.2 Utilisateurs externes, **SUPPRIMER** SécureExt.02 dans son intégralité et **REMPLACER** par ce qui suit :

SécureExt.02	S'assurer de l'authentification des utilisateurs à l'aide des services CléGC ou SecureKey Service de Concierge et d'une seconde composante d'authentification (telle que les secrets partagés) lors de l'ouverture d'une session dans le Service public Web vertical et frontal de la solution.

Changement nº 115 :

Dans la SECTION 5 DE L'ANNEXE A : EXIGENCES RELATIVES À LA SÉCURITÉ DES TI, 1.2 — Exigences détaillées, Catégorie Contrôle d'accès et gestion des comptes, **INSÉRER** ce qui suit :

SC.00.A	L'entrepreneur doit préparer un plan de contrôle de l'accès et de gestion des utilisateurs.

Changement nº 116 :

Dans la SECTION 5 DE L'ANNEXE A, EXIGENCES RELATIVES À LA SÉCURITÉ DES TI, 1.2, Exigences détaillées, **SUPPRIMER** SC.48 dans son intégralité et **REMPLACER** par ce qui suit :

SC.48	L'entrepreneur doit présenter au GC des procédures détaillées d'installation des composants de sécurité. Celles-ci doivent à tout le moins comprendre : (a) les étapes nécessaires à l'installation et à la configuration sécurisées; (b) l'installation et la configuration de l'ensemble des solutions de sécurité technique; (c) la configuration des composants de sécurité des produits matériels; (d) la configuration des composants de sécurité des produits logiciels.

Changement nº 117 :

Dans la SECTION 6 DE L'ANNEXE A, GESTION DES ESSAIS, 1.2 Exigences détaillées, catégorie Gestion des essais (généralités) :

INSÉRER ce qui suit :

TM.00.A	Fournir un plan d'essai préliminaire conformément aux exigences de l'ANNEXE A, section 6. L'entrepreneur doit se fonder sur les exigences opérationnelles et techniques, et l'architecture conceptuelle pour préparer le plan d'essai.

SUPPRIMER entièrement TM.01 et **REMPLACER** par le libellé suivant :

TM.01.A	Avant d'amorcer les travaux de développement, l'entrepreneur doit élaborer la stratégie de la mise à essai. Sous réserve de l'approbation du chargé de projet, la stratégie doit comprendre à tout le moins les renseignements suivants pour chacune des étapes des essais exigés : (a) un aperçu général de la stratégie proposée en ce qui a trait aux essais; (b) un cadre de gestion des défauts; (c) une stratégie d'entrée et de sortie; (d) des rencontres entre le chargé de projet et l'entrepreneur; (e) une stratégie permanente de gestion et d'atténuation des risques.
TM.02.A	L'entrepreneur doit développer un de mise à l'essai qui doit démontrer à tout le moins : A. une prise en considération des exigences en matière de sécurité du Plan d'essai de l'intégration de la sécurité, SC-42, ainsi que de la section 6 de l'ANNEXE A; B. une couverture adéquate des essais pour s'assurer que les exigences clés atteignent l'état de production nécessaire. Prise en considération des points suivants et renvoi à ces derniers : i. un essai d'intégration; ii. des essais fonctionnels et non fonctionnels, notamment les essais de sécurité; iii. des essais de migration des données; iv. un essai d'acceptation par le client. C. La détection et gestion des risques.

INSÉRER ce qui suit :

TM.06.A	Fournir la matrice de traçabilité complète des exigences dûment remplie.

Changement nº 118 :

Dans la SECTION 7 DE L'ANNEXE A, GESTION ET SURVEILLANCE, sous-section 1.3 Exigences détaillées - Gestion de projet, catégorie Plan de projet (généralités) :

SUPPRIMER :

PM.06	L'entrepreneur doit élaborer et tenir à jour un plan de gestion de projet qui doit être conforme aux pratiques exemplaires ou aux normes de l'industrie et approuvé par le chargé de projet.

INSÉRER :

PM.05.A	L'entrepreneur doit fournir un plan préliminaire de gestion de projet qui reflète la stratégie qu'il utilisera pour assurer la mise en œuvre des exigences décrites dans l'ANNEXE A, sections 2 à 7. Le plan doit s'harmoniser avec le cadre du Système national de gestion de projet (SNGP).

PM.06	Élaborer et tenir à jour un plan de gestion de projet qui doit être conforme aux pratiques exemplaires ou aux normes de l'industrie et approuvé par le chargé de projet. Le plan doit satisfaire aux éléments demandés suivants et indiquer la façon dont il favorise l'atteinte des résultats escomptés énoncés dans l'ANNEXE A, sections 1 à 7, y compris : a) le document sur la gouvernance du projet et la structure de l'équipe du projet; b) le plan de gestion de la portée; c) le plan de gestion du calendrier; d) le calendrier de projet; e) le plan de gestion des risques; f) le plan de gestion de la qualité.

Changement nº 119 :

Dans la SECTION 7 DE L'ANNEXE A, GESTION ET SURVEILLANCE, 2.2.2 Plan de gestion des changements, catégorie Généralités :

SUPPRIMER :

CM.02	Le plan de gestion des changements doit être intégré au plan de gestion de projet et au calendrier de projet.
CM.03	L'entrepreneur doit : (a) élaborer des processus et des procédures visant à institutionnaliser le changement; (b) recenser les activités relatives à la gestion du changement et les relier aux divers jalons du projet; (c) harmoniser ses travaux avec les calendriers de formation, les communications et les approches; (d) harmoniser ses travaux avec les calendriers des activités de transition liées à la restructuration des processus; (e) cerner les attentes relatives à l'affectation des ressources liées au changement suivant les étapes et les jalons du projet; (f) déterminer la nature des ressources du GC que nécessitera la gestion du changement, le moment où on fera appel à ces ressources et la période pendant laquelle on les utilisera; (g) déterminer les secteurs présentant des risques élevés qui peuvent avoir des répercussions sur la réussite du changement, élaborer des stratégies d'atténuation, recommander des mesures d'atténuation et transmettre les résultats au GC; (h) trouver des moyens rapides et efficaces de simplifier les activités de gestion du changement; (i) collaborer avec le GC pour exécuter la stratégie et le plan de gestion du changement; (j) mettre en œuvre les activités d'assainissement relatives à la gestion du changement qui seront nécessaires au long du cycle de vie du projet; (k) formuler des recommandations sur la ligne de conduite optimale à adopter pour traiter et résoudre les problèmes propres aux intervenants; (l) appuyer les ressources GC reconnues pour se faire les championnes du changement; (m) assurer la coordination entre les diverses composantes de la gestion du changement et les autres activités du projet.

INSÉRER :

CM.01.A	L'entrepreneur est tenu de fournir un plan préliminaire de gestion du changement, qui comprend, entre autres, les éléments suivants : A. Compréhension approfondie des exigences en matière de gestion des changements; B. Prise en considération des points suivants : i. évitement de l'interruption du service aux Canadiens; ii. facilitation de l'adoption du processus et de la transition terminologique pour tous les utilisateurs finaux, y compris les utilisateurs externes et le personnel interne; iii. utilisation appropriée, conforme et rapide du nouveau système ainsi que l'entrée de données dans le nouveau système; iv. Qualité et intégrité des services fournis. C. Méthode d'évaluation exhaustive pour évaluer l'efficacité des activités de gestion des changements.
CM.02	L'entrepreneur doit préparer un plan de gestion des changements après que le plan préliminaire de gestion des changements ait été évalué par le Canada et qu'il a été jugé comme un soutien approprié à la transition efficace d'un état de départ vers un état ciblé et démontre les exigences énoncées ci-dessus. Le plan de gestion des changements doit être intégré au plan de gestion de projet et au calendrier de projet.
CM.03	L'entrepreneur doit : (a) élaborer des processus et des procédures visant à institutionnaliser le changement; (b) recenser les activités relatives à la gestion du changement et les relier aux divers jalons du projet; (c) harmoniser ses travaux avec les calendriers de formation, les communications et les approches; (d) harmoniser ses travaux avec les calendriers des activités de transition liées à la restructuration des processus; (e) cerner les attentes relatives à l'affectation des ressources liées au changement suivant les étapes et les jalons du projet; (f) déterminer la nature des ressources du GC que nécessitera la gestion du changement, le moment où on fera appel à ces ressources et la période pendant laquelle on les utilisera; (g) déterminer les secteurs présentant des risques élevés qui peuvent avoir des répercussions sur la réussite du changement, élaborer des stratégies d'atténuation, recommander des mesures d'atténuation et transmettre les résultats au GC; (h) trouver des moyens rapides et efficaces de simplifier les activités de gestion du changement; (i) collaborer avec le GC pour exécuter la stratégie et le plan de gestion du changement; (j) mettre en œuvre les activités d'assainissement relatives à la gestion du changement qui seront nécessaires au long du cycle de vie du projet; (k) formuler des recommandations sur la ligne de conduite optimale à adopter pour traiter et résoudre les problèmes propres aux intervenants; (l) appuyer les ressources du GC reconnues pour se faire les championnes du changement; (m) assurer la coordination entre les diverses composantes de la gestion du changement et les autres activités du projet; (n) fournir un plan de services de soutien qui prévoit le transfert de connaissances aux opérations.

Changement n° 120 :

À la SECTION 9 DE L'ANNEXE A, SERVICES FACULTATIFS, **INSÉRER** ce qui suit :

1.8 SERVICES DE SÉCURITÉ SUPPLÉMENTAIRES

En plus des services de sécurité énoncés dans la section 5, Exigences relatives à la sécurité des TI, l'entrepreneur doit fournir sur demande et selon les besoins des services de sécurité des TI supplémentaires et doit proposer des ressources qualifiées et ayant l'expérience de fournir des services de sécurité des TI.

Changement n° 121 :

À l'appendice 2 de l'ANNEXE A — Activités principales, **SUPPRIMER** le calendrier des Activités principales dans son intégralité et **REMPLACER** par ce qui suit :

Activités principales	Date d'achèvement
Attribution du contrat	Août 2017
Planification de la solution et analyse	Décembre 2017
Conception de la solution	Décembre 2017
Communication	Mars 2019 [1]
Essais	Mars 2019 [1]
Formation	Mars 2019 [1]
Développement et configuration de la solution	Août 2018
Préparation opérationnelle	Mars 2019
Mise en œuvre et lancement du projet pilote de solution	Mars 2019
Projet pilote de solution	Juin 2019
Mise en œuvre progressive	Septembre 2019
Stabilisation de la solution et transition de sortie	Décembre 2019
Clôture du projet	Décembre 2019

Changement n° 122 :

À l'appendice 2 de l'ANNEXE A - Activités principales, **SUPPRIMER** 9. **Stabilisation et transition de sortie** dans son intégralité et **REMPLACER** par le libellé suivant :

9. Stabilisation et transition de sortie

Au cours de cette période de neuf (9) mois après le lancement de la solution, l'entrepreneur doit continuer d'assurer un soutien dans tous les domaines liés à la solution décrits à l'ANNEXE A, dont la formation, les communications, la gestion du changement et la correction des défauts. En outre, l'entrepreneur doit assurer une transition harmonieuse des activités de soutien à SPAC pendant cette étape.

L'entrepreneur doit :

(a) fournir un rapport de clôture de projet :
- évaluation du rendement du projet;
- détermination des leçons apprises;

- confirmation que les activités contractuelles essentielles et que les autres activités de clôture du projet ont été menées à bien;
- questions en suspens;
- transfert des biens, des produits livrables et des fonctions administratives en cours.
    - Mesure des avantages/résultats après la mise en œuvre du projet (IRC).

(b) fournir un document rendant compte des enseignements tirés;
(c) effectuer le transfert des connaissances;
(d) fournir des guides de conception portant sur la solution;
(e) fournir toute la documentation concernant la formation, les communications, les processus opérationnels, la gestion du changement et les essais;
(f) fournir des recommandations futures consignées par écrit.

Changement nº 123 :

À l'appendice 3 de l'ANNEXE A — Aperçu des comptes d'utilisateurs, 1. Utilisateurs externes :

SUPPRIMER :

Les clients et partenaires du Secteur de la sécurité industrielle (SSI) qui sont décrits ci-après comme des utilisateurs externes pourront accéder aux services du SSI par l'intermédiaire du portail Web de la solution.

INSÉRER :

Les clients et partenaires du Secteur de la sécurité industrielle (SSI) qui sont décrits ci-après comme des utilisateurs externes pourront accéder aux services du SSI par l'intermédiaire du service public Web vertical et frontal de la solution.

Changement nº 124 :

À l'appendice 5 de l'ANNEXE A — Glossaire :

SUPPRIMER :

Interface intuitive : Interfaces de la solution qui sont intuitives, comme il est défini ci-dessus (« intuitif ») pour les parties de la solution qui portent sur le portail Web et l'application de traitement des services.

Données du système de SSI: I) portail de prestation des services

Portail : page Web spécialement conçue qui réunit les renseignements de diverses sources de manière uniforme. Habituellement, chaque source d'information occupe un endroit prévu à cet effet dans la page; souvent, l'utilisateur peut configurer quels renseignements afficher. Les variantes des portails comprennent des «tableaux de bord» intranet pour les cadres et les gestionnaires.

INSÉRER :

Interface intuitive : Interfaces de la solution qui sont intuitives, comme il est défini ci-dessus (« intuitif ») pour les parties de la solution qui portent sur le service public Web vertical et frontal et l'application de traitement des services.

Données du système du SSI : I) Prestation de services du service public Web vertical et frontal

Service public Web vertical et frontal : page Web spécialement conçue qui réunit les renseignements de diverses sources de manière uniforme. Habituellement, chaque source d'information occupe un endroit prévu à cet effet dans la page; souvent, l'utilisateur peut configurer quels renseignements afficher. Les variantes du service public Web vertical et frontal comprennent des « tableaux de bord » intranet pour les cadres et les gestionnaires.

Changement nº 125 :

SUPPRIMER L'ANNEXE B —Barème de prix dans son intégralité et la **REMPLACER** par l'ANNEXE B — Barème de prix jointe à la présente modification.

Changement nº 126 :

SUPPRIMER L'ANNEXE F —Renseignements sur les catégories pour les Services facultatifs dans son intégralité et la **REMPLACER** par l'ANNEXE F — Renseignements sur les catégories pour les Services facultatifs jointe à la présente modification.

Changement nº 127 :

SUPPRIMER la pièce jointe 1 de la partie 4 — Évaluation technique dans son intégralité et la **REMPLACER** avec la pièce jointe 1 de la partie 4 — Évaluation technique jointe à cette modification.

Changement nº 128 :

SUPPRIMER le formulaire 3 de la partie 4 — Demande de soumissions —Soumission financière dans son intégralité et la **REMPLACER** par le formulaire 3 de la partie 4 — Demande de soumissions — Soumission financière jointe à la présente modification.

B. QUESTIONS

Question nº 164 :

Veuillez expliquer les limites de ce qu'offrent SPC et le service de SPGC sur les exigences présentées dans l'annexe A – Énoncé des besoins, 1.2 Exigences détaillées, à propos de ce qui suit :

a) la gestion de la configuration;
b) la protection des limites et la sécurité;
c) la surveillance.

Réponse nº 164 :

L'énoncé qui suit précise ce qu'offrent la Direction générale du dirigeant principal de l'information (DGDPI) et Services partagés Canada (SPC) en ce qui concerne les exigences présentées dans l'ANNEXE A – Énoncé des besoins, 1.2 Exigences détaillées :

a) La DGDPI prend en charge la gestion de la configuration de la plateforme Dynamics. La DGDPI fournira des locataires de la plateforme Dynamics partagée pour la mise en œuvre de la solution par l'entrepreneur. SPC sera responsable des aspects relatifs à l'infrastructure de la solution de transformation des systèmes de sécurité industrielle (TSSI), comme les machines virtuelles, le stockage et la mise en réseau. L'équipe de projet de TI de Travaux publics et Services gouvernementaux Canada assurera la coordination des activités de mise en œuvre de la solution de l'entrepreneur avec SPC et la DGDPI.
b) La protection des limites fait partie de l'intervention en matière de sécurité relative aux exigences générales en matière de sécurité pour la solution. Comme la protection des limites dans le présent contexte est liée à l'infrastructure de TI fournie par SPC, ce dernier est responsable de cet élément.
c) La surveillance est requise pour deux aspects de la solution; 1) Rendement – la DGDPI et SPC surveillent, de concert, la santé de la plateforme MS Dynamics afin de repérer les problèmes ou les problèmes éventuels, comme la mise à l'échelle. 2) Sécurité – la surveillance constitue une exigence en matière de sécurité aux fins d'intégrité des données au niveau de l'application.

L'entrepreneur sera responsable de toute surveillance requise de la solution de TSSI (au niveau de l'application).

Question nº 165 :

Quelles sont les responsabilités du soumissionnaire et quels éléments, desquels le soumissionnaire peut tirer profit, sont déjà fournis par le service de SPGC et SPC?

Réponse nº 165 :

L'entrepreneur est responsable de l'ensemble de la configuration, du développement et de l'intégration logicielles requis pour la solution de TSSI, au moyen des plateformes et des services offerts, conformément à l'Énoncé des travaux.

SPC est responsable de la prestation et du soutien de l'infrastructure, comme les serveurs, la mise en réseau et le service de courriel.

- L'ensemble du matériel se rattachant à la plateforme de la solution, y compris les serveurs et la connectivité au réseau, entre autres, sera fourni par le gouvernement du Canada.
- Le gouvernement du Canada fournira tous les ensembles de TI cibles.

C'est la DGDPI qui apporte les capacités de gestion des cas au moyen de la plateforme technologique MS Dynamics CRM fondée sur une architecture à locataires multiples.

Le service de la DGDPI comprend les éléments suivants :

- l'infrastructure MS Dynamics pour les activités non liées à la production et liées à la production;
- l'administration et le soutien de la plateforme partagée;
- la gestion des licences Dynamics;
- le modèle de sécurité fédéré facilitant l'intégration aux systèmes pangouvernementaux du gouvernement du Canada;
- l'accréditation de la plateforme pour le degré de sensibilité des données Protégé B, avec disponibilité et intégrité moyennes;
- la surveillance du rendement et des problèmes liés à la plateforme, avec notifications automatiques;
- le ragréage;
- la mise à l'échelle de la plateforme, sur demande;
- la réinitialisation des locataires et la sauvegarde des données;
- l'élaboration de pratiques exemplaires et d'orientations;
- l'intégration et la coordination des flux d'intégration Dynamics avec SPC.

Question nº 166 :

Si un soumissionnaire recommande l'utilisation de produits ne faisant pas partie de « l'ensemble des produits du GC », comment doit-il alors représenter les coûts de licence de ces produits dans leur proposition?

Réponse nº 166 :

Veuillez vous reporter à la réponse à la question n° 204 de la présente modification 011.

Question nº 167 :

À la page 32 de l'annexe A – Énoncé des travaux, SPAC indique que « les logiciels nécessaires à l'entrepreneur, mais qui ne figurent pas dans l'ensemble des produits du GC, doivent être approuvés par le GC avant le début du processus d'installation de TPSGC ». Si un tel produit n'est pas approuvé après l'octroi du contrat, sera-t-il possible de faire une demande de changement pour un remplacement?

Réponse nº 167 :

Veuillez vous reporter à la réponse à la question n° 204 de la présente modification 011.

Question nº 168 :

La DP, notamment la liste de vérification des exigences relative à la sécurité (LVERS), semble permettre aux soumissionnaires et aux sous-traitants étrangers de présenter une soumission dans le cadre de ce processus ou d'y participer. Cette façon de faire semble être en contradiction directe avec la politique et la pratique actuelles du Conseil du Trésor en matière de souveraineté des données, particulièrement pour ce qui est des données de nature délicate du gouvernement et des citoyens comme les renseignements de base fournis pour l'obtention de l'attestation de sécurité d'un particulier, la possession de toutes les attestations de sécurité du gouvernement du Canada au niveau « Secret » et « Très secret » applicables à l'industrie canadienne, ainsi que le traitement de renseignements de nature délicate sur les biens contrôlés et le contrôle de l'exportation.

Des renseignements de base de nature délicate de citoyens canadiens pourraient être exposés à des risques, même si le ou les fournisseurs n'exploitent pas les systèmes, car ils possèdent une connaissance technique approfondie des systèmes utilisés pour traiter, stocker et sauvegarder les données. Lorsque des données sont regroupées à l'échelle nationale dans l'ensemble des domaines fonctionnels indiqués au paragraphe précédent, il pourrait y avoir, selon CGI, une menace réelle à la sécurité nationale (p. ex. le nombre d'individus possédant une attestation au niveau « Très secret » et leur identité, quels sous-traitants sont autorisés à travailler sur quels contrats et pour quels ministères.).

Il est fortement recommandé que, conformément aux pratiques semblables observées récemment, le Canada impose dans le cadre de ce besoin les exclusions suivantes pour motif de sécurité nationale :

a) Tous les soumissionnaires, les partenaires ou les membres d'une coentreprise doivent être membres en règle du programme Participation, contrôle et influence étrangers du gouvernement du Canada;
b) Les sous-traitants doivent continuer de faire l'objet d'une approbation individuelle, conformément au programme du gouvernement du Canada sur la sécurité visant les sous-traitants, compte tenu des exclusions liées à la sécurité dans le cadre de cette DP;
c) Les produits doivent être examinés pour déterminer leur conformité à la politique sur l'intégrité de la chaîne d'approvisionnement canadienne;
d) Le soutien des systèmes et services fournis par les fournisseurs (p. ex. deuxième et troisième niveau) doit être limité au personnel du Canada possédant une attestation au niveau exigé dans la LVERS, à moins d'une approbation précise à titre exceptionnelle par SPAC.

Réponse nº 168 :

En ce qui concerne les points a), b), c) et d), veuillez vous reporter à la réponse à la question nº 5 de la modification 003.

Question nº 169 :

À propos de la Partie 4 de l'Annexe A : Accès sécurisé, 1.2 Exigences détaillées, 1.2.2 Utilisateurs externes, SécureExt.01 (page 38 de 70); pourriez-vous fournir les spécifications d'intégrations pour l'utilisation du service CléGC et SecureKey Service de concierge?

Réponse nº 169 :

Les spécifications d'intégration pour l'utilisation du service CléGC et SecureKey Service de concierge figurent dans la pièce CATS2 jointe dans cette modification 011. L'infrastructure pour les Services vertical web initial destinées au public et l'intégration à la Fédération des justificatifs du gouvernement du Canada (FJGC) devraient être mises en place au moyen du service courant (services de fédération Active Directory).

Question nº 170 :

Pour SC.59 Application du flux d'information :

Dans un environnement d'entreprise, comme celui du gouvernement du Canada, l'application du flux d'information se fait généralement au niveau du périmètre de sécurité par un produit ayant la capacité d'analyser et d'évaluer un contenu, quel que soit son type, afin d'en déterminer l'acceptabilité, et également de détecter les codes malveillants (ce qui peut impliquer une évaluation manuelle par certains groupes chargés de déterminer ce qui est acceptable et ce qui ne l'est pas) :

a) Est-il dans l'intention de cette exigence que le fournisseur propose ce type de produit en tant qu'élément supplémentaire de l'architecture de la solution TSSI ou le fournisseur devrait-il supposer que ce type de plateforme est fourni par le gouvernement comme un logiciel fourni par le gouvernement et qu'il est exploité par SPC?
b) Dans ce dernier cas, le fournisseur devrait-il également supposer que l'exigence consiste à appuyer SPC au niveau de la configuration de la plateforme du gouvernement, laquelle surveille et soutient l'application du flux d'information?
c) Dans le premier cas, de quelle façon le fournisseur devrait-il inclure le nouveau produit? Faut-il supposer que ce produit peut être inséré dans l'infrastructure globale à la périphérie de l'environnement du gouvernement et que le gouvernement fournira une équipe responsable du fonctionnement de cette plateforme? Faut-il résoudre les incidents et réaliser des évaluations manuelles, le cas échéant?

Réponse nº 170 :

Conformément à l'exigence technique Tech.34, l'entrepreneur doit concevoir l'architecture physique. Cette conception comprendra les interfaces pour toutes les composantes comprises connues, les partenaires tiers, etc. (des détails sur les exigences relatives à l'interface se trouvent dans l'exigence technique Tech.38).

a) L'entrepreneur sera uniquement responsable des contrôles de sécurité mise en œuvre dans le logiciel de la solution et toutes les procédures connexes qui relèvent de la portée du projet de l'entrepreneur. L'entrepreneur devra mener une analyse des lacunes au moment de l'attribution du contrat et formulera des recommandations au gouvernement du Canada. L'entrepreneur devra aider à mettre en œuvre et à configurer toute solution logicielle.

b) L'entrepreneur devra soutenir la configuration du gouvernement du Canada et toute plateforme de ce dernier qui fait partie de l'architecture physique du Secteur de la sécurité industrielle (SSI).

c) Pour en savoir plus, veuillez vous reporter à la réponse à la question nº 204 de la présente modification.

Question nº 171 :

Dans SC.23 Surveillance du système d'information, SPAC exige ce qui suit :

« La solution doit :

a) pouvoir détecter les attaques, les indicateurs d'attaques potentielles, ainsi que les réseaux locaux et les connexions à distance non autorisés; et
b) informer les administrateurs de la sécurité de ces détections. »

Dans le même temps, à la page 57 de l'« ANNEXE A – Énoncé des travaux », SPAC indique ce qui suit :

« La solution est mise en œuvre par l'entrepreneur à l'aide de l'infrastructure que lui fournit Services partagés Canada (SPC) : serveurs, réseaux, bases de données, etc. SPC travaille en collaboration avec l'entrepreneur et assume les responsabilités suivantes, sans pour autant s'y limiter : i. concevoir et mettre en œuvre l'infrastructure qui soutient la solution et en permet la réalisation; »

Nous souhaiterions obtenir une clarification sur le rôle de SPC dans la mise en œuvre de SC.23. Étant donné que SPC est responsable de l'infrastructure réseau spécialisée capable de mettre en œuvre les fonctions de sécurité décrites dans SC.23, l'Entrepreneur est-il tenu de collaborer avec SPC pour veiller à ce que cette infrastructure appuie la solution et s'y intègre, ou l'Entrepreneur est-il tenu de dupliquer dans la solution les fonctions fournies par SPC?

Réponse nº 171 :

La conception de la solution doit inclure la surveillance du système d'information décrite dans SC.23. L'entrepreneur doit inclure cela dans les architectures physique et logique, comme il est décrit dans l'exigence technique Tech.34. Ces architectures doivent être conçues en fonction de l'architecture conceptuelle de la TSSI et comprendront les spécifications de tous les composants des plateformes et des services de la solution TSSI. TPSGC fournira du soutien à l'entrepreneur en facilitant l'accès aux renseignements requis que l'entrepreneur ne peut pas obtenir autrement et dont il a besoin pour réaliser les produits livrables.

Question nº 172 :

Dans la PIÈCE JOINTE 1 DE LA PARTIE 4 – CRITÈRES D'ÉVALUATION TECHNIQUE, 3. CRITÈRES OBLIGATOIRES, le critère O1 contient la clause d'exigence volumétrique suivante :

« Aux fins de la présente évaluation, un projet similaire serait défini comme un projet ayant au moins 35 % du nombre d'utilisateurs, de comptes, de transactions et de types de transactions indiqués à l'annexe A, section 1, 3.1, Données volumétriques. »

Les données volumétriques donnent les indications suivantes :

Type d'utilisateur	PSC – Industrie	PSC – Gouvernement	Total PSC	Total PSG	Total des comptes	35 %
Comptes d'utilisateurs internes			396	91	487	170
Comptes d'utilisateurs externes	161 000	905	161 905	22 000	183 905	64 367
Total de utilisateurs			162 301	22 091	184 392	
				35 %	64 537	

a) Dans l'Annexe A – Énoncé des travaux, Section 1 : Aperçu de la solution de sécurité industrielle du canada, 3.1 Données volumétriques (page 9 de 70) fait référence aux comptes d'utilisateurs internes et externes, mais n'explique pas la différence entre « nombre d'utilisateurs » et « nombre de comptes ». Les termes « nombre d'utilisateurs » et « nombre de comptes » devraient-ils s'interpréter de manière identique? Dans le cas contraire, SPAC pourrait-il préciser la différence entre ces deux termes?

b) Pour nous, le « nombre total d'utilisateurs et le nombre total de comptes » dans les projets cités en référence devraient être d'au moins 35 % des comptes d'utilisateurs internes et externes (c.-à-d. 184 392 * 35 % = 64 537 utilisateurs). Notre interprétation est-elle correcte?

c) Si nous respectons la condition b) ci-dessus (c.-à-d. 64 537 utilisateurs internes et externes), est-il également nécessaire d'avoir 170 comptes d'utilisateurs internes (487 * 35 %) pour se qualifier?

d) Si nous respectons la condition b) ci-dessus (c.-à-d. 64 537 utilisateurs internes et externes), est-il également nécessaire d'avoir 64 367 comptes d'utilisateurs externes (183 905 * 35 %) pour se qualifier?

e) Étant donné que le projet a été conçu, élaboré, mis en œuvre et remis au client afin d'assumer la poursuite des opérations avant l'enregistrement des utilisateurs, le nombre actuel d'enregistrements n'est pas connu car nous n'avons plus accès au système. En outre, le nombre d'enregistrements et le volume de transactions relèvent de la propriété du client et sont considérés comme confidentiels. Il est donc impossible pour nous de fournir ces renseignements. SPAC pourrait-il envisager de supprimer cette exigence ou de fournir des estimations générales du volume prévu ou imparti?

Réponse nº 172 :

Comme il est précisé dans la réponse à la question 38 de la modification 004, les projets cités en référence du soumissionnaire doivent répondre à 65 % des données volumétriques indiquées à l'Annexe A, section 1, partie 3.1.

L'État est disposé à accepter des données volumétriques utilisées dans la conception et le développement plutôt qu'une confirmation des données volumétriques réellement utilisées dans le cadre du projet cité en référence dans une capacité après la mise en œuvre. En d'autres termes, si la solution a été conçue et développée pour desservir un volume escompté d'utilisateurs, un nombre d'opérations et un éventail d'opérations qui répondent aux données volumétriques demandées pour répondre aux critères O1 et O2,

le projet peut être cité en référence. Il convient de noter que les volumes prévus doivent être demeurés supérieurs aux données volumétriques indiquées tout au long de la durée du projet.

Veuillez vous reporter à la modification 127 et aux réponses aux questions nº 202 et nº 216 de la présente modification 011.

Question nº 173 :

Dans la PIÈCE JOINTE 1 DE LA PARTIE 4 – CRITÈRES D'ÉVALUATION TECHNIQUE, 3. CRITÈRES OBLIGATOIRES, le critère O2 contient la clause d'exigence volumétrique suivante :

« Aux fins de la présente évaluation, un projet similaire serait défini comme un projet ayant au moins 35 % des données volumétriques indiquées à l'annexe A, section 1, 3.1, Données volumétriques. » Plus précisément, le nombre d'utilisateurs, le nombre de comptes, ainsi que le nombre et la diversité des transactions ».

a) SPAC pourrait-il préciser les conditions nécessaires afin de se qualifier pour le « nombre de transactions »? Est-il fait référence au volume de transactions d'enregistrement ou de transactions d'application?

b) SPAC pourrait-il préciser les conditions nécessaires afin de se qualifier pour la « diversité de transactions »? Quels seraient les critères de qualification pour une autre application similaire, mais pas totalement identique à celle de SPAC? Comment une application différente prenant en charge différents types de cas peut-elle s'inscrire dans le cadre de ce critère de « diversité des transactions »? Une liste de types de cas de GRC serait-elle suffisante? Comment cela sera-t-il évalué? Dans de nombreux cas, nous n'avons pas connaissance du volume de transactions étant donné qu'après la réussite de la mise en œuvre, nous n'avons plus accès au système. En outre, le volume de transactions relève de la propriété du client et est bien souvent considéré comme confidentiel. Il est donc impossible pour nous de fournir ce renseignement. SPAC pourrait-il envisager de supprimer cette exigence ou de fournir une description générale du volume prévu?

Réponse nº 173 :

Par éventail d'opérations, on entend différents secteurs d'activité abordés dans la même solution. Ces secteurs d'activité peuvent varier par différents groupes d'intervenants, divers types de circuits de travail ou d'activités menées, etc.

Veuillez vous reporter à la modification 127 et aux réponses aux questions nº 172, nº 202 et nº 216 de la présente modification 011 pour en savoir plus sur la présentation des données volumétriques.

Question nº 174 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.01 (page 45 de 77) « (a) imposer à chaque utilisateur des contrôles d'accès fondés sur le rôle ».

Le Canada souhaite-t-il que les contrôles d'accès fondés sur le rôle ou le service d'annuaire (p. ex., Active Directory) fournis par le soumissionnaire soient entièrement indépendants ou est-il prévu que la solution du soumissionnaire utilise les contrôles d'accès fondés sur le rôle et les services d'annuaires existants du Canada?

Réponse nº 174 :

L'entrepreneur devra configurer la solution en vue de fournir les contrôles d'accès fondés sur le rôle (comme il est indiqué dans APP-OPS.01), en tirant parti des services d'annuaire internes existants du gouvernement du Canada, au besoin, plutôt que de créer de nouveaux annuaires. L'entrepreneur devra déterminer les exigences qui peuvent être satisfaites au moyen de l'infrastructure d'annuaire existante destinée aux utilisateurs externes.

Question nº 175 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.09 (page 47 de 77).

L'entrepreneur doit :

a) documenter rigoureusement tous les liens existant entre les systèmes de TI, notamment la description des données, le flux de données, les exigences et les mécanismes liés à la sécurité et à l'accès, le rendement, les attentes touchant la fiabilité, etc.
b) fournir la preuve que les fournisseurs de services informatiques externes se conforment aux exigences de contrôle de la sécurité informatique de l'organisation et utilisent des contrôles de sécurité conformément à la Norme de sécurité et de gestion des marchés du SCT.

Question/Commentaire

a) Le soumissionnaire n'a aucune connaissance ni responsabilité en ce qui a trait à l'architecture de réseau dans l'environnement d'hébergement ou dans les flux de données et ne dispose d'aucune capacité de sécurité externe à la solution fournie. Le Canada envisagera-t-il de modifier l'exigence comme suit : « documenter rigoureusement tous les liens existant entre les systèmes de TI, notamment la description des données, le flux de données, les exigences et les mécanismes liés à la sécurité et à l'accès, le rendement, les attentes touchant la fiabilité, etc., internes à la solution fournie, ainsi que les dépendances externes quant aux systèmes et à la sécurité »?

b) Le fournisseur de service n'est pas l'opérateur de la solution et ne constitue pas non plus son environnement d'hébergement; par conséquent, il n'a aucun contrôle sur les services externes de système d'information et n'a aucune visibilité de ceux-ci. Le Canada pourrait-il clarifier cette exigence afin qu'elle soit conforme à la portée du rôle du fournisseur ou la supprimer?

Réponse nº 175 :

Conformément aux exigences opérationnelles relatives au groupe d'interconnectivité (APP-ICN.01-.10), l'entrepreneur est responsable de la conception, de la fabrication et de la documentation des interfaces (Tech.38) de façon à ce que celles-ci soient conformes aux exigences. Même s'il n'est pas responsable de l'infrastructure, l'entrepreneur sera responsable de concevoir et de configurer les composants de l'architecture conceptuelle afin de rendre possibles les processus opérationnels nécessaires tout en veillant à ce que les bons contrôles de sécurité connexes aient été pris en compte et intégrés. TPSGC fournira du soutien à l'entrepreneur en lui facilitant l'accès aux renseignements requis qu'il ne peut pas se procurer autrement et dont il a besoin pour la réalisation des livrables.

Question nº 176 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.11 (page 47 de 77).

L'entrepreneur doit évaluer l'incidence des changements sur la sécurité s'il procède à la mise en œuvre de nouveaux logiciels, à un important changement de configuration ou à la gestion des correctifs. Son évaluation comportera les points suivants :

a) analyse des nouveaux logiciels avant leur installation dans un environnement opérationnel afin de déterminer les répercussions sur la sécurité attribuables aux failles, aux points faibles, à l'incompatibilité ou à la malveillance intentionnelle;
b) communication à TPSGC de l'incidence possible sur la sécurité des changements avant leur mise en œuvre;
c) vérification des fonctions de sécurité après les changements pour s'assurer qu'elles ont été mises en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités quant au respect des exigences pertinentes en matière de sécurité.

Le soumissionnaire n'est ni l'autorité opérationnelle en matière de sécurité, ni l'autorité opérationnelle, ni le gestionnaire des changements opérationnels pour la solution après sa livraison et sa mise en service. Le Canada envisagera-t-il de supprimer cette exigence?

Réponse nº 176 :

L'entrepreneur doit répondre aux exigences de SC.16, après l'attribution du contrat. Si, après l'attribution du contrat, l'information du gouvernement du Canada n'est pas facilement accessible, le gouvernement du Canada aidera l'entrepreneur à obtenir les renseignements requis. Il n'y a aucune obligation à fournir de la documentation de type architecture de sécurité de l'information (autre que pour R4) avant l'attribution du contrat.

Question nº 177 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.16 (page 48 de 77). L'entrepreneur doit, dans le cadre de la solution, consigner l'architecture de sécurité de l'information en respectant les paramètres suivants :

a) décrire globalement la philosophie, les exigences et l'approche qu'il prévoit adopter relativement à l'information afin d'assurer la confidentialité, l'intégrité et l'accès;
b) décrire la façon dont il assurera l'intégration et le soutien de l'architecture de sécurité de l'information à l'architecture d'entreprise;
c) décrire toute hypothèse relative à la sécurité de l'information qui porterait sur les services externes et tout lien de dépendance à l'égard de ceux-ci.

L'architecture de l'environnement qui héberge le système d'application relève du GC (et non du soumissionnaire). Pour cette raison, il serait très difficile pour le soumissionnaire de décrire les nombreux points requis dans la réponse à cette exigence (p. ex. tout aspect détaillé de l'architecture d'entreprise).

On recommande de demander que les soumissionnaires fournissent une architecture ou une topologie générale de la sécurité et d'y joindre des annotations narratives illustrant la façon dont le système du soumissionnaire serait déployé et sécurisé dans une architecture d'entreprise conforme aux normes du GC (p. ex., ITSG-22, ITSG-38). Après l'attribution du contrat, le soumissionnaire peut fournir une architecture d'entreprise plus détaillée au niveau des applications qui examine l'intégration de la sécurité dans l'environnement d'entreprise d'hébergement, pour autant que ces détails soient fournis à ce moment par le GC.

Le Canada envisagera-t-il de modifier cette exigence conformément à la recommandation ci-dessus?

Réponse nº 177 :

L'entrepreneur doit répondre aux exigences de SC.16, après l'attribution du contrat. Si, après l'attribution du contrat, l'information du gouvernement du Canada n'est pas facilement accessible, le gouvernement du Canada aidera l'entrepreneur à obtenir les renseignements requis. Il n'y a aucune obligation à fournir de la documentation de type architecture de sécurité de l'information (autre que pour R4) avant l'attribution du contrat.

Question nº 178 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.17 (page 48 de 77). L'entrepreneur doit fournir la conception générale d'une solution en matière de sécurité qui comporte à tout le moins :

a) Un schéma général des composants qui illustre clairement la répartition des services et des composants dans les zones de sécurité du réseau et qui établit les principaux flux de données liés à la sécurité;
b) Les couches de l'architecture (p. ex. communication, virtualisation, plateforme/système d'exploitation, gestion des données, intergiciels, applications opérationnelles);
c) Une description des mesures de défense du périmètre de la zone du réseau;
d) Une description de l'utilisation des technologies de virtualisation, s'il y a lieu;
e) Une description de la répartition de l'ensemble des exigences de sécurité technique dans les éléments de la conception générale des services, et ce, pour toutes les couches de l'architecture;
f) Une description de la répartition de l'ensemble des exigences de sécurité non technique au sein des éléments organisationnels ou opérationnels généraux;
g) Une description de l'approche relativement à :
   i. la gestion à distance;
   ii. le contrôle d'accès;
   iii. la gestion et la vérification de la sécurité;
   iv. la gestion de la configuration;
   v. la gestion des correctifs.
h) Une justification des principales décisions concernant la conception.

Cette exigence pourrait faire l'objet d'une interprétation allant considérablement au-delà de la portée du rôle du soumissionnaire. On recommande qu'elle soit modifiée pour préciser « dans la portée de la solution » afin de définir plus précisément les limites de la portée.

Le Canada envisagera-t-il de modifier cette exigence conformément à la recommandation ci-dessus?

Réponse nº 178 :

Comme il est indiqué dans la réponse à la question 170 de la présente modification, l'entrepreneur doit fournir une architecture physique dans le cadre des livrables. Cette structure doit comporter les caractéristiques techniques de tous les composants de la solution. L'entrepreneur doit fournir la conception générale d'une solution en matière de sécurité en fonction de l'architecture physique en se concentrant sur la portée de la solution qui lui a été assignée.

Question nº 179 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.17 (page 48 de 77). L'entrepreneur doit fournir la conception générale d'une solution en matière de sécurité qui comporte à tout le moins :

a) Un schéma général des composants qui illustre clairement la répartition des services et des composants dans les zones de sécurité du réseau et qui établit les principaux flux de données liés à la sécurité;
b) Les couches de l'architecture (p. ex. communication, virtualisation, plateforme/système d'exploitation, gestion des données, intergiciels, applications opérationnelles);
c) Une description des mesures de défense du périmètre de la zone du réseau;
d) Une description de l'utilisation des technologies de virtualisation, s'il y a lieu;
e) Une description de la répartition de l'ensemble des exigences de sécurité technique dans les éléments de la conception générale des services, et ce, pour toutes les couches de l'architecture;
f) Une description de la répartition de l'ensemble des exigences de sécurité non technique au sein des éléments organisationnels ou opérationnels généraux;
g) Une description de l'approche relativement à :
   i. la gestion à distance;
   ii. le contrôle d'accès;
   iii. la gestion et la vérification de la sécurité;
   iv. la gestion de la configuration;
   v. la gestion des correctifs.
h) Une justification des principales décisions concernant la conception.

Conformément au point SC.17, il incombe uniquement au soumissionnaire de fournir une application ou un système sécuritaire. La sécurité et la conception de l'environnement d'hébergement relève du GC. Même s'il devra donner des conseils sur l'emplacement et les interfaces sécuritaires et adéquats, le soumissionnaire ne devrait pas être le principal responsable des éléments suivants, mais devait uniquement fournir un soutien à leur égard :

- l'architecture de sécurité d'entreprise;
- la gestion de la sécurité opérationnelle;
- la gestion des correctifs, ou la gestion des changements opérationnels.

On recommande que la portée de cette recommandation soit revue pour tenir compte des observations. Le cas échéant, le soumissionnaire peut donner des conseils sur ces éléments, mais il ne sera pas responsable des éléments allant au-delà de la portée de son rôle. Le Canada envisagera-t-il de modifier cette exigence pour préciser les éléments dont le soumissionnaire est responsable et ceux pour lesquels il est tenu de fournir un soutien?

Réponse nº 179 :

L'entrepreneur sera responsable de la mise en œuvre des contrôles dans la solution logicielle, et de toutes les procédures à l'appui. Si l'entrepreneur n'est pas en mesure d'appliquer un contrôle, il aidera le gouvernement du Canada à le mettre en œuvre et à le répertorier.

Quels que soient les contrôles que l'entrepreneur doit mettre en œuvre, il lui incombe de les répertorier tous pendant la conception de l'architecture physique, y compris tous les composants de l'ensemble de la solution. La conception générale d'une solution en matière de sécurité prend en charge et renseigne l'architecture, à mesure qu'elle reconnaît les contrôles de sécurité et où ils sont appliqués.

La conception générale d'une solution en matière de sécurité prend également en charge la conception détaillée d'une solution en matière de sécurité (exigence SC.18), qui contient des renseignements détaillés sur les contrôles de sécurité des composants de la solution fournis par l'entrepreneur.

L'architecture physique, la conception générale d'une solution en matière de sécurité et la conception détaillée d'une solution en matière de sécurité sont comprises dans la portée des travaux de l'entrepreneur et seront prises en charge par le gouvernement du Canada.

Question nº 180 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.18 (page 49 de 77). L'entrepreneur doit fournir la conception détaillée d'une solution en matière de sécurité qui comporte à tout le moins :

a) Un schéma détaillé des composants (il doit s'agir d'une version approfondie du schéma général des composants);
b) Une description de la répartition des mécanismes de sécurité technique au sein des éléments de la conception détaillée des services;
c) La description de l'association des mécanismes de sécurité non technique aux éléments de la conception générale qui concernent l'organisation ou les opérations;
d) Une justification des principales décisions concernant la conception.

Reportez-vous aux observations formulées à la question 98. Le schéma exigé est habituellement décrit comme un schéma topographique de sécurité de troisième couche axé sur le réseau, accompagné d'un document fournissant des descriptions annotées de l'ensemble des constructions et les protections liées à la sécurité, y compris une description de la façon dont la totalité des exigences de sécurité technique seront respectées.

Le Canada envisagera-t-il de modifier cette exigence pour préciser les éléments dont le soumissionnaire est responsable et ceux pour lesquels il est tenu de fournir un soutien?

Réponse nº 180 :

L'entrepreneur doit produire une conception détaillée d'une solution en matière de sécurité à partir de la conception générale d'une solution en matière de sécurité (SC.17) pour la solution telle qu'elle est conçue par l'entrepreneur qui en est responsable. La conception détaillée d'une solution en matière de sécurité doit aborder tous les contrôles de sécurité connexes pour la solution conçue. Veuillez vous reporter à la réponse aux questions 170 et 178 de la présente modification pour obtenir de plus amples renseignements.

Question nº 181 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.19 (page 49 de 77). La solution doit :

a) Être mise en œuvre de manière à résister aux attaques entraînant un refus de service afin d'atteindre la disponibilité cible du SSI;
b) Comporter des dispositifs de surveillance et de contrôle à ses limites extérieures (connexions Internet et GC);
c) Être configurée de manière à refuser la communication par défaut et à ne permettre que les communications autorisées;
d) Pouvoir détecter et refuser les communications qui semblent constituer une menace pour les systèmes internes et externes, et attribuer ces communications à une personne dans toute la mesure du possible;
e) Protéger l'authenticité des sessions de communication;
f) Annuler les identifiants de session lors de la fermeture de la session ou de tout autre type de déconnexion;

g) Utiliser des identificateurs de session unique et ne reconnaître que les identificateurs générés par le système.

Certains filtres de trafic et autres protections discriminatoires peuvent être mis en œuvre dans la solution. Cependant, ceux-ci dépendront également des pare-feux d'entreprise, des services d'information et de distribution et d'autres systèmes conçus et exploités par l'autorité de l'environnement d'exploitation et de l'autorité de gestion de la sécurité (SPC).

Le Canada envisagera-t-il de modifier cette exigence pour préciser les éléments dont le soumissionnaire est responsable et ceux pour lesquels il est tenu de fournir un soutien?

Réponse nº 181 :

L'entrepreneur, pendant la création de l'architecture physique, présentera des spécifications liées à l'intégration pour les dispositifs qui font partie de la conception, mais qui sont réputés se trouver à l'extérieur de la portée de la solution soutenue par l'entrepreneur. Au moment de créer l'architecture, l'entrepreneur doit tenir compte des exigences liées au contrôle de sécurité et indiquer si elles devraient être mises en œuvre. Si l'entrepreneur détermine qu'il doit ajouter d'autres composantes à la solution afin de répondre aux exigences liées au contrôle, on s'attend à ce qu'il formule une recommandation et à ce qu'il mette en œuvre ces contrôles une fois que le gouvernement du Canada les aura approuvés. L'entrepreneur sera responsable de soutenir ou d'aider à soutenir le gouvernement du Canada dans l'appui à la solution pendant la durée du contrat.

Question nº 182 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.20 (page 49 de 77). La solution doit s'interrompre par mesure préventive en cas de défaillance des dispositifs de protection des limites.

Il s'agit habituellement du réglage par défaut de tous les pare-feux et de tous les dispositifs de protection des frontières assurant la sécurité. Ainsi, la plupart des systèmes auxquels cette exigence s'applique seraient fournis par le GC (p. ex. pare-feux de zone et de zone d'accès public). La seule exception viserait les pare-feux hébergés internes à la solution.

Le Canada envisagera-t-il de supprimer cette exigence ou de la modifier pour préciser la responsabilité du soumissionnaire?

Réponse nº 182 :

Selon cette exigence, la solution doit s'interrompre par mesure de sécurité en réponse à un dispositif de protection des limites. Dans son commentaire et sa question, l'auteur affirme qu'il s'agit du réglage par défaut de la plupart des dispositifs de protection des limites. Il ne s'agit pas du contrôle requis. L'entrepreneur doit s'assurer que la solution (celle conçue par l'entrepreneur) s'interrompt par mesure de sécurité.

Question nº 183 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.23 (page 50 de 77). La solution doit :

a) Pouvoir détecter les attaques, les indicateurs d'attaques potentielles, ainsi que les réseaux locaux et les connexions à distance non autorisés;
b) Informer les administrateurs de la sécurité de ces détections.

Cette exigence devrait relever de l'autorité opérationnelle ainsi que de l'autorité opérationnelle en matière de sécurité.

Le soumissionnaire peut collaborer avec ces dernières pour veiller à ce que les capacités adéquates en matière de détection et de surveillance soient incluses. Cependant, la surveillance et les avis vont au-delà de la portée du rôle du soumissionnaire. Le Canada envisagera-t-il de supprimer cette exigence ou de la modifier pour préciser la responsabilité du soumissionnaire?

Réponse nº 183 :

L'entrepreneur travaillera avec le GC pour s'assurer que les mesures appropriées ont été mises en place afin de détecter les incidents et d'en faire le suivi. Prenez note qu'il est spécifié à SC.23 que c'est la solution qui doit être en mesure d'aviser les administrateurs de la sécurité.

En ce qui a trait aux obligations de l'entrepreneur de signaler les incidents relatifs à la sécurité et à la protection des renseignements personnels - conformément à SC.33, l'entrepreneur doit aviser le GC en créant un billet d'incident de sécurité.

Question nº 184 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.26 (page 50 de 77). L'entrepreneur doit consigner chacun des ports et des protocoles nécessaires à la solution. Ce document doit comprendre à tout le moins :

(a) le port, le protocole ou le service utilisé;
(b) une description de l'information transférée dans ce port, ce protocole ou ce service;
(c) une description du flux (source et destination);
(d) les règles relatives au pare-feu ou à l'acheminement nécessaires au soutien de la communication.

Les règles textuelles relatives aux pare-feux à présenter dépendront du type de dispositifs de protection des frontières utilisées par l'autorité opérationnelle. Habituellement, une description de flux précisant notamment l'origine, la destination, les ports et protocoles et le chiffrement est fournie. Les politiques relatives aux pare-feux se fondent ensuite sur celle-ci. Le Canada envisagera-t-il de modifier l'exigence ou de fournir l'information ci-dessus?

Réponse nº 184 :

Les Services vertical web initial destinées au public et les pare-feu associés seront configurés par SPC dans le cadre de la fourniture de services d'approvisionnement et de soutien de l'infrastructure. À l'obtention de l'approbation, il incombe à l'entrepreneur de présenter à SPC la conception des Services vertical web initial destinées au public, les autorisations requises et les exigences relatives aux pare-feu, y compris les ports et les protocoles pour la mise en œuvre.

Question nº 185 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.37 (page 51 de 77). L'entrepreneur doit, pour la durée du contrat, créer un ou plusieurs dossiers d'incident pour chaque incident relevé.

La surveillance de la sécurité de la solution lorsque celle-ci est fonctionnelle ne relève pas du soumissionnaire. Le Canada pourrait-il clarifier ce que signifie cette exigence?

Réponse nº 185 :

Des incidents visés par le point SC.37 peuvent ou non provenir de la solution logicielle ou être détectés par un examen des fichiers journaux. Pour la durée du contrat, tout processus ou toute activité, y compris toute interaction avec les utilisateurs qui entraîne une situation contraire au résultat prévu, nécessitera la production d'un billet d'incident. Une fois le billet d'incident créé, l'entrepreneur sera tenu d'enquêter à l'égard de tout incident associé à la solution qu'il aura préparée. Si l'entrepreneur ne dispose pas d'un accès, il travaillera avec le gouvernement du Canada pour déterminer la cause de l'incident.

Question nº 186 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.38 (page 51 de 77). L'entrepreneur doit, pour la durée du contrat, apporter son appui et son aide au GC pour le maintien du niveau de sécurité de la solution en s'employant constamment à relever les problèmes suivants et à en informer le GC :

a) Les menaces et les vulnérabilités;
b) Les activités malveillantes et les accès non autorisés.

La surveillance de la sécurité de la solution lorsque celle-ci est fonctionnelle ne relève pas du soumissionnaire. Le Canada pourrait-il clarifier ce que signifie cette exigence?

Réponse nº 186 :

On s'attend à ce que l'entrepreneur surveille la solution pendant toute la durée du contrat, ce qui comprend, sans toutefois s'y limiter, l'examen de fichiers journaux afin de relever des activités imprévues. Si les éditeurs du logiciel utilisé dans le cadre de la solution, le client opérationnel ou l'entrepreneur découvrent et signalent des menaces, des vulnérabilités ou des incidents nouveaux, l'entrepreneur doit aider le gouvernement du Canada à évaluer les risques que les menaces ou les vulnérabilités posent pour la solution. Cela comprend la conformité à SC.37, s'il y a lieu.

Question nº 187 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.39 (page 52 de 77). L'entrepreneur doit élaborer un plan d'atténuation des vulnérabilités de la solution approuvé par TPSGC dans les cinq jours ouvrables suivant l'achèvement d'une évaluation de la vulnérabilité : le plan propose des mesures de protection pour atténuer les risques ciblés dans cette évaluation.

Cet aspect relève habituellement de l'autorité opérationnelle de TI, en collaboration avec l'autorité de sécurité. Les fournisseurs de solutions peuvent fournir des conseils et une rétroaction à l'appui, conformément au point SC.36.

Le Canada pourrait-il préciser et corriger l'exigence, conformément aux points SC.32, 33, 34, 36, 37 et 38?

Réponse nº 187 :

L'évaluation des vulnérabilités de la solution doit se faire au cours du cycle de conception du projet, avant la sortie de la version finale. Conformément à la réponse à la question 58 de la modification 008, l'entrepreneur concevra la solution à partir de l'architecture physique et décrira les contrôles de sécurité qui relèvent de l'entrepreneur (description détaillée) et qui ne relèvent pas de lui (description générale). L'entrepreneur aidera le gouvernement du Canada dans l'évaluation des vulnérabilités visées par la portée limitée du projet de l'entrepreneur. Le plan d'atténuation est requis cinq jours après la réalisation de

l'évaluation des vulnérabilités pour tout composant relevant de l'entrepreneur. La mise en œuvre de toute mesure d'atténuation des vulnérabilités pourrait nécessiter la collaboration de l'entrepreneur avec le gouvernement du Canada. Le point SC.36 parle des activités associées aux incidents et non de l'évaluation des vulnérabilités.

Question nº 188 :

Dans l'annexe A – Énoncé des travaux, section 5 : Exigences relatives à la sécurité de la TI, 1.2 Exigences détaillées, SC.70 (page 56 de 77). La solution doit mettre en œuvre l'authentification multifactorielle pour permettre au réseau d'accéder :

a) Aux comptes privilégiés;
b) Aux comptes non privilégiés.

L'authentification multifactorielle nécessite habituellement l'émission (et la gestion) de jetons matériels ou logiciels en plus d'un mot de passe. Elle peut entraîner certains coûts et n'est pas habituellement utilisée au sein du GC pour les comptes publics et non privilégiés.

Le Canada pourrait-il indiquer exactement les types de comptes et les rôles qui nécessiteraient une authentification multifactorielle?

Le Canada pourrait-il confirmer que le système de TSSI effectuerait l'authentification en fonction d'un système d'authentification du GC externe à l'application?

Réponse nº 188 :

Dans le cadre de la restructuration des pratiques commerciales, on s'attend à ce que l'entrepreneur détermine les exigences liées à l'authentification et au contrôle de l'accès pour chaque rôle d'utilisateur, en fonction des contrôles de sécurité indiqués pour la désignation du profil de sécurité PB/M/M. Se reporter aux contrôles IA 2 et IA 5 de la modification nº 3 de la demande de propositions pour en savoir plus sur la gestion des accès. Se reporter à la réponse à la question nº 169 de la présente modification pour en savoir plus sur les exigences liées au service d'authentification.

Question nº 189 :

Dans la structure de données :

Une évaluation de la QUALITÉ a-t-elle été réalisée sur les fichiers de données sources? Puisque l'entrepreneur ne travaillera qu'avec les fichiers de données échantillons, le client a-t-il récemment effectué une évaluation de qualité sur les données sources RÉELLES? Dans la négative, à quand remonte la dernière évaluation de la qualité?

Réponse nº 189 :

Veuillez consulter la réponse à la question 111 dans la modification 008.

Question nº 190 :

TPSGC pourrait-il nous remettre une copie du schéma de l'architecture du module RA illustrant tous les tableaux qui existent actuellement (y compris leur structure principale)?

Réponse nº 190 :

Aucune architecture de renseignements d'affaires (RA) n'est actuellement disponible étant donné que l'environnement de RA n'a pas encore été établi pour le projet de TSSI. Veuillez vous reporter à la réponse à la question nº 119 de la modification 008 pour en savoir plus à ce sujet.

Question nº 191 :

Quelle est la fréquence de mise à jour (fréquence de régénération) de l'entrepôt de données et des dépôts de données?

Réponse nº 191 :

Comme aucun environnement de renseignements d'affaires (RA) n'est mis sur pied pour le projet de TSSI, ces précisions ne peuvent être données pour l'instant. Veuillez vous reporter à la réponse à la question nº 190 de la présente modification.

Question nº 192 :

TPSGC pourrait-il fournir le schéma des tâches d'extraction, de transformation et de chargement (ETC) existantes (de la source à la cible) et indiquer l'outil utilisé dans l'exécution de ces scripts d'ETC?

Réponse nº 192 :

Aucun diagramme des tâches d'extraction, de transformation et de chargement (ETC) ne doit être fourni, puisque tous les rapports sont produits au moyen des anciens systèmes opérationnels ou dans le cadre de requêtes spéciales directes dans la base de données. Au moment de déterminer les exigences relatives à l'établissement de rapports pour le projet de TSSI et de cerner une solution RA, le soumissionnaire devra proposer des scripts d'ETC pour maintenir les données RA. Pour en savoir plus sur les outils ETC, veuillez vous reporter à la question nº 67 de la modification nº 006. Par contre, veuillez vous reporter à la question nº 204 dans cette modification 011 en ce qui concerne l'approvisionnement de logiciel. Pour en savoir plus sur l'environnement RA, veuillez consulter la réponse à la question nº 190 de la présente modification.

En ce qui concerne la migration de données, on s'attend à ce que l'entrepreneur conçoive des scripts pour assurer la migration des données à partir des anciennes sources de données. Veuillez vous reporter aux exigences relatives à la migration de données indiquées dans la section 2 de l'ANNEXE A.

Question nº 193 :

Énoncé des travaux nº SC.23 – Veuillez confirmer que l'État souhaite que l'entrepreneur fournisse des technologies de détection d'attaque et de notification en plus des technologies de sécurité de TPSGC et de SPC déjà en place.

Réponse nº 193 :

L'entrepreneur doit tirer parti des technologies de détection et de signalement d'attaque en place et offertes actuellement au gouvernement du Canada et cerner les secteurs où elles ne répondent pas aux exigences.

Veuillez vous reporter à la réponse à la question nº 204 de la présente modification pour en savoir plus.

Question nº 194 :

Dans la modification nº 3, l'État a changé le niveau d'intégrité de la solution, le faisant passer de moyen à élevé. Il s'agit d'un changement important des exigences des contrôles de sécurité, particulièrement en ce qui concerne le degré d'automatisation requis par les contrôles supplémentaires indiqués dans cette modification. De plus, la réponse de l'État à la question 18 indique que les entrepreneurs ne doivent pas présumer que les voies existantes d'échange de données respectent les exigences relatives à la sécurité. L'État en est conscient, mais ce changement important apporté aux exigences et cette réponse augmentent le niveau de risque d'une solution complexe et la probabilité des retards pouvant toucher de nombreux autres intervenants, qui pourraient ne pas être mesure de respecter des exigences de niveau élevé en matière d'intégrité.

Pendant la conférence des soumissionnaires, l'État a indiqué que son budget pour ce projet se situait entre six et onze millions de dollars. Toutefois, compte tenu de la révision du profil d'intégrité de la solution, l'État a-t-il vérifié les répercussions de sa décision sur son budget, autant pour les dépenses uniques que pour les coûts d'entretien à long terme? Le cas échéant, l'État a-t-il avisé les fournisseurs du changement du budget?

Réponse nº 194 :

Le Canada a examiné les exigences relatives au prix de lot ferme total et a fait passer la limite inférieure de 6 000 000,00 à 8 000 000,00 $. La limite supérieure demeure la même. Veuillez vous reporter au changement 128 de la présente modification 011.

Question nº 195 :

En ce qui concerne l'exigence SC.19, elle indique que « la solution doit être mise en œuvre de manière à résister aux attaques entraînant un refus de service afin d'atteindre la disponibilité cible du SSI. » En ce qui a trait à cette exigence :

a) Quels sont les objectifs de disponibilités du SSI? Ils ne sont pas mentionnés dans la demande de proposition.
b) Quels sont les critères relatifs à l'objectif de point de rétablissement et à l'objectif de délai de rétablissement?

Réponse nº 195 :

Conformément à l'évaluation des répercussions opérationnelles réalisée en matière de systèmes de sécurité industrielle et au plan de continuité des activités :

a) La disponibilité ciblée dans le cadre de la TSSI est la suivante : le système doit être disponible 99,35 % du temps.
b) Les critères liés à l'objectif de point de reprise (OPR) et à l'objectif de délai de rétablissement (ODR) sont respectivement de 8 à 14 jours (niveau 2) et de 1 heure.

Question nº 196 :

Conformément à la modification nº 3, l'énoncé suivant est inclus au point 1.2 de l'article 5 figurant dans l'ANNEXE A du changement 39 (page 7 de 18) : « Ça sera la responsabilité de l'entrepreneur d'intégrer tous les contrôles de sécurité, y compris ceux rencontrés par TPSGC, SSC et l'entrepreneur dans la matrice de traçabilité des exigences relatives à la sécurité. »

Question : Étant donné qu'il est possible que cette modification puisse entraîner un risque ou une dépendance sur lesquels l'entrepreneur n'a aucune maîtrise, l'État peut-il clarifier les points suivants?

(a) L'entrepreneur doit-il saisir des explications dans la matrice de traçabilité des exigences en matière de sécurité pour souligner la façon dont TPSGC et SPC respectent les exigences des contrôles qui ne lui incombent pas? Le cas échéant, comment l'entrepreneur peut-il rapidement obtenir ces renseignements?

(b) L'entrepreneur sera-t-il indemnisé de toute responsabilité relative à la conformité qui ne relève pas de sa portée ou sur laquelle elle n'a aucune emprise?

(c) Et comment l'entrepreneur sera-t-il protégé ou rémunéré dans l'éventualité où l'autorisation d'exploitation est retardée en raison de la non-conformité de SPC ou de SPAC (situation que l'entrepreneur ne contrôle pas)?

Réponse nº 196 :

L'entrepreneur doit inclure dans le document de la matrice de traçabilité des exigences relatives à la sécurité tous les contrôles de sécurité qu'il aura déterminés dans l'architecture physique. L'entrepreneur ne peut avoir en sa possession les documents complets du GC en ce qui concerne les contrôles de sécurité assurés par le GC, mais cela doit être indiqué dans la matrice de traçabilité des exigences relatives à la sécurité.

a) L'entrepreneur présentera des explications sur ses contrôles de sécurité qu'il aura mis en œuvre, et il ajoutera tout renseignement disponible auprès de TPSGC et de SPC en ce qui concerne les contrôles qui ne sont pas visés par la portée de la mise en œuvre qui incombe à l'entrepreneur.
b) Le Canada n'indemnisera pas l'entrepreneur, sauf lorsque cela est approprié.
c) Veuillez vous reporter à l'article 2035 10 – Retard justifiable des Conditions générales - besoins plus complexes de services du Guide des clauses et conditions uniformisées d'achat.

Question nº 197 :

D'autres changements seront-ils apportés à l'article 5 : Sécurité de la technologie de l'information?

Réponse nº 197 :

Veuillez vous reporter aux changements nº 115 et nº 116 de cette modification 011. Aucun autre changement n'est prévu pour la section 5 de l'annexe A durant tout le processus de demande de propositions. Toutefois, si des changements doivent être apportés, ils seront communiqués dans une modification officielle.

Question nº 198 :

L'exigence APP-IM.27 indique ce qui suit : « Permet aux utilisateurs internes de récupérer les enregistrements archivés d'un dossier de cas pendant une période donnée. »

Les « enregistrements archivés » comprennent-ils les dossiers tenus dans le système actuel SSI ainsi que les dossiers tenus dans les systèmes des partenaires (p. ex., GRC) qui font référence à un cas passé? Ou comprennent-ils seulement les dossiers qui seront tenus dans la solution future (y compris les dossiers tenus dans GCDOCS)?

Réponse nº 198 :

En ce qui a trait à APP-IM.27, les archives ne contiennent pas ceux tenus dans les systèmes du Secteur de la sécurité industrielle existants ou dans les systèmes des partenaires qui font référence à un cas passé. Ils ne font référence qu'aux dossiers qui seront tenus dans la solution future. Pour plus de précisions sur l'information qui sera tenue dans la solution future, veuillez consulter la réponse à la question nº 88 dans la modification 007.

Question nº 199 :

Nous demandons par la présente que la date d'échéance des questions soit modifiée pour qu'elle ait lieu cinq jours avant la clôture des soumissions.

Réponse nº 199 :

Le Canada ne modifiera pas l'article 2.3 Demandes de renseignements – en période de soumission de la partie 2 de la demande de propositions.

Question nº 200 :

Dans l'appendice 2 de l'annexe A (Activités principales), le calendrier indique que les jalons « Planification et analyse » et « Conception de la solution » sont des activités principales. La plupart de nos domaines de travail (p. ex., mise à l'essai ou formation) ne peuvent pas réaliser leur planification, leur analyse ou leur conception avant que la solution soit presque totalement mise au point et en œuvre.

La première activité principale, soit « Planification et analyse », peut-elle être renommée « Planification de la solution et analyse »? Il ne serait alors pas nécessaire de terminer les domaines de travail en aval pour effectuer la planification, l'analyse et la conception d'ici décembre 2017. Ces étapes devront fort probablement être modifiées et révisées dans la deuxième moitié de 2018, soit après que la solution est conçue et presque totalement mise au point.

Réponse nº 200 :

À des fins de clarté, le calendrier des jalons a été modifié comme suggéré de façon à s'intituler « Activités principales ». Veuillez vous reporter au changement nº 121 de cette modification 011. Pour plus de renseignements concernant les activités principales, veuillez consulter la réponse à la question nº 154 de la modification nº 009.

Question nº 201 :

De nombreuses exigences de l'annexe A ont changé. SPAC peut-il publier à nouveau l'intégralité de l'annexe A, à laquelle les diverses modifications ont été apportées, afin de veiller à ce que le fournisseur tienne compte des exigences les plus récentes dans sa réponse?

Réponse nº 201 :

L'annexe A a été mise à jour pour indiquer tous les changements apportés jusqu'à maintenant et elle est jointe à la présente modification 011.

Question nº 202 :

Pièce jointe 1 de la partie 4, O1; modification 004, changement nº 49 – Il est entendu que le Canada cherche des soumissionnaires possédant de l'expérience et de l'expertise en matière de restructuration des processus opérationnels (RPO) et de gestion du changement dans le cadre de grands projets ou de

projets complexes. Cela dit, la complexité des initiatives de RPO et de gestion du changement dans le cadre de grands projets est attribuable au changement et aux effets que cela entraînera sur l'environnement opérationnel des clients, ainsi que sur leurs employés – non pas sur les données volumétriques.

Il est demandé que l'exigence O1 relative aux données volumétriques soit supprimée et remplacée par un indicateur d'envergure et de complexité plus pertinent, tel que la valeur monétaire du projet.

Il est par ailleurs demandé que la conformité à l'exigence relative aux données volumétriques indiquées à la modification 004, changement nº 49, soit mesurée de manière cumulative en tenant compte de tous les projets de référence présentés pour répondre au critère O1.

Réponse nº 202 :

Le Canada évaluera les projets de référence des soumissionnaires afin de s'assurer que leur envergure et leur portée correspondent à celles de l'initiative de TSSI. Les données volumétriques demandées aux critères O1 et O2 servent de base de référence pour cette évaluation en indiquant :

- le nombre de clients internes et externes (comptes);
- le volume de transactions qui seront traitées dans la solution fournie (volumes transactionnels);
- les différents secteurs d'activités visés (diversité).

Le Canada croit qu'un projet de TI assorti de toutes les données volumétriques demandées peut servir d'indicateur mesurable des activités de gestion du changement et de restructuration des processus opérationnels qui auraient été nécessaires.

En ce qui concerne l'addition des données volumétriques de divers projets, le Canada ne croit pas que l'exigence relative à ces données devrait être satisfaite de façon cumulative par plusieurs des projets de référence, et ne modifiera donc pas l'évaluation technique à cet égard.

Toutefois, O1 et O2 ont été modifiés. Veuillez vous reporter au changement nº 127, et aux réponses aux questions nº 172 et nº 216.

Question nº 203 :

Pièce jointe 1 de la partie 4, O2; modification 004, changement nº 51 – Comme il a été indiqué à la conférence des soumissionnaires, le Canada souhaite tirer profit de l'expertise qui se trouve dans l'industrie afin soutenir cette initiative. L'expérience des grands intégrateurs de systèmes dont souhaite profiter le Canada a été acquise dans le cadre de nombreux grands projets.

Le critère O2, selon lequel tous les projets de référence doivent respecter l'exigence relative aux données volumétriques, est strict et il limite la capacité du soumissionnaire à démontrer son expérience diversifiée et autrement pertinente. Il est demandé que l'exigence soit révisée de sorte que « au moins un (1) des trois (3) » projets de référence respecte l'exigence relative aux données volumétriques – ce qui est compatible avec les autres composantes du critère O2.

Il est par ailleurs demandé que la conformité à l'exigence relative aux données volumétriques indiquées à la modification 004, changement nº 49, soit mesurée de manière cumulative en tenant compte de tous les projets de référence présentés pour répondre au critère O2.

Réponse nº 203 :

Veuillez vous reporter à la réponse à la question 202 de la présente modification.

Question nº 204 :

Le 28 avril 2017, nous avons posé à SPAC les questions suivantes :

- En examinant les besoins en fonction de l'architecture de la solution, nous constatons qu'il peut y avoir des lacunes qui nécessiteront l'intégration et la configuration d'autres produits afin de minimiser la complexité et les coûts des solutions, tout en maximisant la valeur pour le Canada. Quelle approche l'industrie devrait-elle adopter selon SPAC pour recommander des solutions, en plus des efforts déployés pour l'intégration et la configuration de la solution, en vue de répondre à l'ensemble des besoins?
- SPAC demande à l'entrepreneur « de concevoir, de développer, de configurer, de tester, de mettre en œuvre, de déployer et de stabiliser la solution, comme l'illustre la figure 2 » de l'annexe A – Énoncé des travaux. Ensuite, SPAC indique que « les suites mentionnées auxquelles l'entrepreneur doit se conformer comprennent » les produits précisés à la page 31 de l'annexe A – Énoncé des travaux. Par ailleurs, la DP autorise « les logiciels nécessaires à l'entrepreneur, mais qui ne figurent pas dans l'ensemble des produits du GC ». Le terme « ensemble des produits du GC » se rapporte-t-il aux produits offerts dans l'AAALL du GC ou aux produits précisés à la page 31 de l'annexe A – Énoncé des travaux?

Jusqu'à présent, nous n'avons pas reçu de réponse aux questions susmentionnées. En outre, les modifications subséquents ont accru le besoin de produits qui ne sont pas indiqués à la section 3, Exigences techniques, comme suit :

La modification 003, changement nº 32, a supprimé le Adxstudio Portal de la section 3, Exigences techniques, tout en indiquant : « Le portail Web sera utilisé par des utilisateurs externes dotés de fonctions et de pouvoirs définis. L'entrepreneur devra fournir et configurer une technologie qui sera hébergée sur le réseau du GC, s'intégrera de manière transparente avec l'application Dynamics CRM, sera extensible pour répondre à la croissance à venir, utilisera les services Web et tirera principalement parti de la configuration plutôt que de la personnalisation. »

En vertu du terme « fournir » dans le paragraphe précédent, il incombe à l'entrepreneur d'acquérir la technologie de portail. Quelles modalités du présent contrat définissent la manière dont l'entrepreneur devrait fournir la technologie de portail?

Réponse nº 204 :

Par souci de clarté, le Canada exige à l'entrepreneur d'offrir les services professionnels et le logiciel prévus à la référence 4007 du guide des Clauses et conditions uniformisées d'achat (CCUA). Pendant la livraison initiale ou à l'étape de préproduction du projet, le Canada n'acquerra pas un logiciel sous licence, comme prévu aux clauses 4003 ou 4004 du manuel des CCUA. Le Canada palliera toute lacune ou se procurera tout logiciel commercial requis pendant la période du contrat, à même ses fournitures existantes, ou de fournitures acquises au moyen de la méthode d'approvisionnement qu'il juge appropriée à ce moment.

Le terme « ensemble des produits du gouvernement du Canada » a été retiré de l'ANNEXE A de l'Énoncé des travaux. Veuillez consulter le changement nº 113 de la présente modification.

Question nº 205 :

En ce qui a trait à la section 6 : Gestion des essais, sous-section 1.2 Exigences détaillées, Catégorie – Gestion des essais (type d'essai), TM09, veuillez fournir une définition de « Mise à l'essai de l'analyse du cheminement » dans le présent contexte.

Réponse nº 205 :

La définition de l'analyse de cheminement ou (l'analyse de la base ou de la direction générale) dans le présent contexte est une méthode permettant de déterminer les essais en fonction des chemins (ou flux) pouvant être effectués dans le système. Il existe des preuves indiquant que la majorité des erreurs sont détectées lors de la première exécution d'un énoncé et l'essai des chemins permet d'obtenir les meilleures possibilités d'exposer ces erreurs.

Question nº 206 :

Dans la modification 003 et dans des modifications subséquentes, le Canada a ajouté des exigences à la DP (p. ex., les contrôles de sécurité dans la modification 003 et les licences de logiciels dans la modification 006). Le changement des exigences ajoute des coûts et des efforts, néanmoins l'enveloppe financière de six à onze millions de dollars demeure inchangée. Nous craignons que le Canada ait établi un « plancher » artificiel pour les propositions financières, compte tenu particulièrement des exigences additionnelles indiquées dans les modifications. Nous savons d'expérience que les fournisseurs se sentent incités à réduire la portée des exigences ou à supprimer autant d'exigences que possible afin d'atteindre le « plancher » de six millions de dollars, puis qu'ils se servent du processus de contrôle des changements pour négocier une augmentation du prix proposé après l'attribution du contrat. Compte tenu de la modification des exigences et afin d'assurer la conformité, nous demandons respectueusement que l'enveloppe financière soit dorénavant de neuf à treize millions de dollars afin que la partie 4 du formulaire 3 de la soumission financière concernant le prix de lot ferme se lise comme suit.

« 2.1 En ce qui concerne les travaux décrits à l'ANNEXE A – ÉNONCÉ DES TRAVAUX, sections 1 à 8, le soumissionnaire doit proposer un prix de lot ferme et un calendrier des étapes clés, conformément au TABLEAU 1 ci-dessous. Le prix de lot ferme total ne doit pas être inférieur à 9 000 000 $ et ne doit pas dépasser 13 000 000 $. Les prix doivent être indiqués en devises canadiennes, ils comprennent les droits de douane, auxquels il faut ajouter les taxes applicables. »

Réponse nº 206 :

Veuillez vous reporter à la réponse à la question nº 194 de la présente modification 011.

Question nº 207 :

La réponse à la question nº 67 concernant la modification 006 de la DP indique que l'entrepreneur doit acquérir et fournir les licences au GC dans le cadre du contrat. Conformément à la section 1.2 Exigences détaillées, l'exigence SC.12 indique que l'entrepreneur doit permettre uniquement l'exécution des logiciels autorisés, déterminés par l'entrepreneur et approuvés par TPSGC, dans la solution. L'exigence de détenir la licence au nom de l'État n'a pas été précisée auparavant et représente un changement important à la DP. Nous signalons en outre que les tableaux financiers dans la DP ne comprennent pas le prix des licences de logiciels.

Nous craignons que l'ajout de nouvelles exigences en matière de logiciel modifie fondamentalement la nature de la DP et que cela impose aux soumissionnaires l'exigence de négocier des licences afin de répondre à la DP. Afin de résoudre ce problème, le Canada pourrait décider de fournir les produits logiciels mentionnés dans la modification 006 (Kingsway and Scribe) à titre d'équipement fourni par le gouvernement (EFG). Aussi demandons-nous respectueusement que ces produits logiciels (plus précisément, Kingsway et secrétaire) soient fournis à titre d'EFG ou que les soumissionnaires puissent répondre aux exigences d'extraction, de transfert et de charge (ETC) au moyen de SQL Server Integration Services (SSIS) avec des API.

Réponse nº 207 :

APP-DM.04 a été modifié afin de préciser le rôle de l'entrepreneur dans d'autres activités de migration de données. En ce qui concerne les produits logiciels, consulter la question nº 204 de la présente modification.

Question nº 208 :

La DP et les clauses du contrat subséquent ne permettent pas aux fournisseurs de fournir les licences des logiciels, en vertu des modalités de ce contrat éventuel. De plus, la modification 006, réponse 67, contredit l'énoncé suivant : « L'entrepreneur doit acquérir et fournir les licences au GC dans le cadre du contrat ». En outre, le tableau des prix, le budget actuel et le schéma d'évaluation financière ne permettent pas aux entrepreneurs d'indiquer le prix des logiciels fournis. L'État peut-il indiquer ses attentes et donner des directives claires sur la manière dont les entrepreneurs devraient proposer et fournir des licences de logiciel, compte tenu des restrictions susmentionnées?

Réponse nº 208 :

Veuillez vous reporter à la réponse à la question nº 204 de la présente modification.

Question nº 209 :

La modification 8, changement 86 entraîne R10.C, qui comprend un tableau des exigences de l'énoncé des travaux, auxquelles il faut répondre en indiquant « prêt à l'emploi » ou « besoin de configuration ». L'énoncé des travaux de la TSSI définit « configurable » comme suit : paramètres pouvant être modifiés et fonctionnalités prêtes à l'emploi sans devoir être personnalisées, pour répondre aux normes et aux exigences de services du gouvernement du Canada, notamment en matière d'architecture des TI, de fonctions, de rendement, de disponibilité, de maintenabilité, de sécurité, de continuité des activités et de reprise après sinistre. Comme la plupart des fonctionnalités prêtes à l'emploi nécessiteront un certain degré de configuration (comme il est indiqué ci-dessus), veuillez envisager de remplacer « besoin de configuration » par « besoin de personnalisation ». Cela reflète davantage l'objectif de l'exigence cotée, à savoir que les fonctionnalités prêtes à l'emploi (qui exigent généralement de la configuration) ne nécessitent pas de modification ni de développement pour répondre aux exigences. S'il est nécessaire de procéder à du développement ou à une modification pour se conformer à cette exigence, les fonctionnalités prêtes à l'emploi seraient considérées ayant un « besoin de personnalisation ».

Réponse nº 209 :

Veuillez vous reporter à la réponse à la question nº 210 de la présente modification.

Question nº 210 :

La modification 8, changement 83, entraîne l'exigence obligatoire O3 Projets de l'entreprise cités en référence : la solution fondée sur un logiciel commercial exige de démontrer que la technologie a la capacité de satisfaire aux exigences mentionnées dans les sections 2, 3 et 4 de l'énoncé des travaux dans l'annexe 1. La section 2 précise trois ensembles de fonctionnalités qui ne sont pas directement liées à la solution de portail Web fondée sur un logiciel commercial : la restructuration des processus opérationnels (série BR.xx), l'application de traitement du service (série APP-xx pour l'automatisation, le soutien opérationnel, l'expérience utilisateur, la gestion de l'information, les communications, le travail sans papier, l'interconnectivité, la production de rapports et l'analyse) et la migration des données (APP-MD.xx). Les exigences fonctionnelles réelles de la solution de portail Web fondée sur un logiciel commercial figurent au

paragraphe 2.2.2, Portail Web (série WP.xx) et les exigences techniques figurent dans la section 3, exigences techniques 48 à 55.

Afin de préciser la portée de la réponse du soumissionnaire relative à la solution de portail Web proposée, fondée sur un logiciel commercial, est-ce que SPAC peut confirmer qu'en vertu de l'exigence obligatoire O3 Projets de l'entreprise cités en référence, la solution fondée sur un logiciel commercial devrait démontrer que la technologie a la capacité de satisfaire aux exigences mentionnées dans la section 2 – Exigences opérationnelles, paragraphe 2.2.2, Portail Web (WP.xx) et dans la section 3 – Exigences techniques, paragraphe 1.2 (exigences techniques 48 à 55)? Ces précisions permettront au soumissionnaire de centrer ses réponses sur les exigences réelles de la solution de portail Web fondée sur un logiciel commercial et simplifieront le processus d'évaluation du gouvernement du Canada.

Réponse nº 210 :

Le Canada a remplacé le terme « portail Web commercial » par « Services vertical web initial destinées au public » dans l'ANNEXE A et dans l'évaluation technique afin d'être moins normatif et de donner une plus grande latitude au soumissionnaire dans la proposition d'une solution.

Par conséquent, les exigences O3 et C10 ont été supprimées et l'évaluation technique a fait l'objet de révisions.

Veuillez consulter le changement nº 127 de la présente modification.

Question nº 211 :

La section R1 c) de la demande de propositions énonce ceci : « Pour chaque activité et chaque étape du projet, les produits livrables connexes, y compris le chemin critique utilisé pour réaliser ces derniers [...] ».

L'État acceptera-t-il le calendrier de projet de Microsoft fourni pour l'exigence R1 d), qui contient la liste des tâches à exécuter dans l'ordre pour réaliser chacune des activités et des étapes du projet, comme une démonstration du chemin critique à emprunter pour réaliser les produits livrables et les étapes en question? Si l'État préfère recevoir ces renseignements sous une autre forme, veuillez fournir un exemple illustrant en détail la façon dont ces renseignements doivent être présentés.

Réponse nº 211 :

Le Canada acceptera la présentation du calendrier demandé dans le critère C1 (d) dans un format de calendrier Microsoft Project.

Question nº 212 :

Dans R1, l'État indique que « le soumissionnaire devrait fournir un plan préliminaire de gestion de projet qui reflète la stratégie qu'il utilisera pour assurer la mise en œuvre des exigences décrites dans l'**ANNEXE A, sections 2 à 7** ».

De plus, l'État indique que : « Le Canada évaluera le plan de gestion du projet proposé par le soumissionnaire, selon le degré auquel il satisfait aux éléments demandés suivants et la façon dont il favorise l'atteinte des résultats escomptés indiqués dans l'**ANNEXE A, sections 1 et 7** ».

L'État pourrait-il confirmer que l'évaluation de la réponse du fournisseur sera fondée sur l'ANNEXE A, sections 2 à 7?

Réponse nº 212 :

Veuillez remarquer que le Canada considère que le plan préliminaire de projet devrait illustrer une stratégie qui réussira à mettre en œuvre les exigences énoncées de 2 à 7, tout en contribuant à l'atteinte des résultats décrits dans les sections 1 et 7. Ces résultats comprennent notamment la section 1, 1.1.2.1 et 1.1.2.2 et la section 7, 2.1, le paragraphe qui affirme « Une gestion du changement efficace vise à : »

Question nº 213 :

Dans la modification 8, changement nº 83, l'État a ajouté une nouvelle exigence O3, comme suit :

Projets de référence de l'entreprise : solution fondée sur un logiciel commercial

L'énoncé des travaux indique les exigences relatives à la technologie de la solution de portail Web fondée sur un logiciel commercial. Le soumissionnaire doit fournir une description complète de la technologie de la solution de portail Web, fondée sur un logiciel commercial, qui sera installée dans les locaux du gouvernement du Canada, notamment les éléments suivants :

a) Produit et version;
b) Exigences relatives aux serveurs;
c) Exigences relatives aux bases de données;
d) Capacité d'intégration avec Microsoft Dynamics (sur place) 2015 ou une version plus récente.

La réponse doit également démontrer que la technologie proposée peut satisfaire aux exigences citées dans les sections 2, 3 et 4 de l'annexe 1.

Le titre de cette exigence, « Projets de l'entreprise cités en référence », présuppose que nous devons fournir une référence de projet, mais l'exigence en tant que telle demande uniquement une description complète de la solution de portail fondée sur un logiciel commercial.

L'État pourrait-il confirmer que la réponse à l'exigence obligatoire O3 requiert uniquement la description de la solution fondée sur un logiciel commercial proposée et qu'elle ne requiert pas de référence de projet?

Réponse nº 213 :

Le critère d'évaluation O3 a été supprimé de l'évaluation technique. Veuillez consulter la réponse à la question n° 210 de la présente modification pour en savoir plus.

Question nº 214 :

Dans la modification 8, changement 83, l'État a ajouté une nouvelle exigence obligatoire O4, comme suit :

Références de client

Pour chaque projet de référence présenté dans les réponses aux exigences obligatoires O1, O2 et O3, le soumissionnaire doit remplir le formulaire 2 jusqu'à la partie 4. Il est possible de communiquer avec la personne-ressource du client afin de valider les renseignements indiqués dans la réponse du soumissionnaire, conformément à la partie 4.2.4, Vérification des références.

Comme l'exigence obligatoire O3 ne requiert pas de référence de projet, l'État pourrait-il modifier l'exigence O4 pour exclure O3?

Réponse nº 214 :

Le critère O4 a été mis à jour à la suite de la suppression du critère d'évaluation O3. Veuillez vous reporter à la réponse à la question nº 210 de la présente modification pour en savoir plus.

Question nº 215 :

Dans le formulaire 3 jusqu'à la partie 4, l'État a demandé que le prix de lot ferme total ne soit pas inférieur à 6 000 000 $. Dans la publication initiale de la demande de propositions, l'État prévoyait fournir tous les logiciels nécessaires à la mise en œuvre de la solution. Toutefois, dans la modification 8, l'État demande au soumissionnaire de fournir la technologie logicielle du portail. Comme les soumissionnaires devront engager ces frais supplémentaires pour fournir la solution, nous demandons à l'État de modifier le prix de lot ferme total minimum à 7 000 000 $.

De plus, selon la pratique courante, le Canada se conforme aux modalités d'octroi de licences de logiciels établies par l'éditeur, car il sera l'utilisateur final. Le Canada peut-il indiquer la méthode en vertu de laquelle il se conformera à ces modalités? Sinon, les fournisseurs ne pourront pas inclure de logiciels supplémentaires, car les modalités d'octroi de licences ne peuvent pas être acceptées par le fournisseur au nom du Canada, ni être assignées au Canada après-coup, en totalité ou en partie.

Réponse nº 215 :

Veuillez vous reporter aux réponses données aux questions nº194 et nº204 dans la présente modification 011.

Question nº 216 :

Les exigences en matière de nombres pour O1 (le nombre de comptes utilisateur, de transactions et de transactions différentes) nous empêchent de nous servir de certains de nos projets cités en référence ayant plusieurs similitudes compatibles et de nombreux points communs appropriés avec les exigences des projets de transformation des systèmes de sécurité industrielle (TSSI) pour les solutions et services de restructuration des processus opérationnels et de gestion du changement. Ces projets de l'entreprise cités en référence sont clairement conformes à toutes les autres exigences O1 et critères d'évaluation et démontrent pleinement nos capacités et notre aptitude à fournir les services de restructuration des processus opérationnels et de gestion du changement pour les projets comme la TSSI. Par conséquent, nous demandons que le critère O1 soit modifié pour qu'il soit exigé que deux projets de l'entreprise cités demandés par O1 au lieu de trois respectent les exigences de nombre prescrites, ce qui permettra tout de même de démontrer le degré et le niveau de rendement antérieur exigé pour la TSSI.

Réponse nº 216 :

L'État modifiera les critères O1 et O2 pour demander deux projets respectant les exigences de nombre plutôt que trois. Les soumissionnaires auront toujours l'obligation de présenter trois projets au total. Veuillez consulter le changement nº 127 et la réponse à la question nº 172 de la présente modification.

Question nº 217 :

Nous sommes en train de réaliser un examen, une vérification et une révision de l'estimation de nos efforts pour l'exécution du projet de TSSI à la lumière des exigences de l'énoncé des travaux de l'Annexe A de la demande de propositions. Services publics et Approvisionnement Canada (SPAC) pourrait-il nous indiquer son raisonnement justifiant la fourchette de prix de 6 à 11 millions de dollars pour la prestation du projet à

prix fixe sur 29 mois, afin que nous puissions harmoniser la portée et les dimensions du projet en conséquence?

Réponse nº 217 :

Veuillez remarquer que la limite inférieure du prix de lot ferme total a été élevée à huit millions de dollars afin de correspondre aux changements en matière de contrôles de l'intégrité élevée. Veuillez vous reporter à la réponse à la question 194 de la présente modification 011. Le soumissionnaire a la responsabilité de proposer une solution qui respecte les besoins financiers, tout en ajustant la portée du projet aux exigences décrites dans l'énoncé des travaux et en rationalisant les coûts d'après des paramètres tels que le niveau d'efforts et le nombre de ressources. Le Canada a déjà mené l'activité qu'il demande aux soumissionnaires d'accomplir, et il en est arrivé à une enveloppe entre 8 et 11 millions de dollars.

Question nº 218 :

SPAC pourrait-il nous confirmer que les quatre options de six mois pour la durée initiale du contrat ne sont pas liées au tableau de prix de lot fermes, mais seulement au tableau de prix des travaux sur demande pour la proposition financière?

Réponse nº 218 :

Le Canada confirme que le tableau prix de lot ferme n'est pas lié aux quatre périodes optionnelles de six mois, ni aux travaux sur demande. L'entrepreneur doit livrer les exigences reliées au prix de lot ferme dans la période de contrat originale de 29 mois.

Question nº 219 :

À propos de la demande de propositions pour la transformation des systèmes de sécurité industrielle (EP243-170549/B), modification 008, question et réponse 110, l'État pourrait-il confirmer qu'aucun lien ne sera fourni pour permettre l'essai à distance des données hors production?

Réponse nº 219 :

Il n'est pas prévu d'établir un lien à distance vers l'environnement Dynamics. L'accès à distance afin de mettre à l'essai la solution de Services vertical web initial destinées au public devrait être une exigence normale.

Question nº 220 :

La modification 003, changement 21 stipulait : « 7.4.7 Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la participation, le contrôle et l'influence étrangers (PCIE) ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut accéder, sans en avoir l'autorisation, à des biens ou à des renseignements INFOSEC. Travaux publics et Services gouvernementaux Canada (TPSGC) déterminera si le statut « Sans PCIE » ou « Avec PCIE » doit être attribué à l'entreprise de l'entrepreneur. Si le statut « Avec PCIE » est attribué à l'entreprise, TPSGC déterminera si des mesures d'atténuation existent ou doivent être prises par l'entreprise afin qu'elle puisse obtenir le statut « Sans PCIE par atténuation ».

L'État peut-il confirmer que les soumissionnaires n'ont pas à déposer ce questionnaire avec leur soumission, et sinon, TPSGC pourrait-il fournir ce questionnaire avant la clôture des soumissions de façon à nous permettre de le remplir et de nous conformer à cette exigence avant l'attribution du contrat?

Réponse nº 220 :

Le Canada confirme qu'il n'est pas nécessaire de soumettre le questionnaire d'évaluation de PCIE avec la soumission avant la date de clôture. Veuillez noter que la réponse à la question 160 dans la modification 009 présentait une erreur. Le questionnaire et les documents connexes doivent être soumis sur demande avant l'attribution du contrat. Par souci de clarté, veuillez vous reporter au paragraphe 7.4.7 de la Partie 7 – Clauses du contrat subséquent.

Question nº 221 :

Dans la modification 008, le Canada a ajouté deux nouvelles exigences portant sur la technologie de portail, les exigences O3 et C10. Les exigences contenues à C10 sont exhaustives puisque celle-ci cote plus de six exemples de mise en place du portail proposé, et qu'elle compare aussi des exigences prêtes à l'emploi à des exigences de configuration. Puisque le Canada a réduit l'exigence à uniquement l'expérience sur le portail avec la solution de portail proposée, cela pourrait forcer les soumissionnaires à cibler jusqu'à six nouveaux justificatifs d'identité avant la clôture de la soumission, ce qui est dispendieux et n'était probablement pas l'intention du Canada.

La technologie et l'expérience de portail faisaient déjà partie des exigences O1 et O2. Nous suggérons de réviser le critère C10 pour qu'on y trouve un maximum de deux exemples avec la solution proposée. Nous croyons qu'il s'agit d'une démonstration suffisante d'expérience, et que cela est juste étant donné le temps disponible avant la date de présentation des soumissions.

À titre indicatif, la révision que nous proposons modifierait l'exigence C10 de la façon suivante :

« Pièce jointe 1 de la partie 4, Critères d'évaluation technique, 4. Critères cotés :

« INSÉRER »

C10 - Solution de portail Web fondée sur un logiciel commercial

En se fondant sur la solution de portail Web fondée sur un logiciel commercial proposée en réponse au critère O3, le soumissionnaire devrait indiquer si la technologie de portail proposée a été mise en place de façon réussie sur d'autres solutions, si elle a un modèle d'octroi de licences et si elle est dotée de fonctionnalités prêtes à l'emploi suffisantes pour remplir les exigences de l'énoncé des travaux, ou s'il faudrait la configurer davantage afin d'y ajouter des fonctionnalités supplémentaires.

A. Le soumissionnaire devrait démontrer qu'il a réussi à mettre en place une technologie de portail dans d'autres projets cités en référence. Les soumissionnaires doivent remplir le formulaire 2 jusqu'à la partie 4 pour tous les projets cités en référence indiqués en réponse au critère C10, puisqu'un maximum de deux projets de référence doit être associé à la solution de portail. Il est possible qu'on communique avec la personne-ressource du client afin de valider les renseignements indiqués dans la réponse du soumissionnaire, conformément à la partie 4.2.4, Vérification des références.

B. Le soumissionnaire devrait décrire le modèle d'octroi de licences proposé, notamment en ce qui a trait au renouvellement, au soutien et à l'assurance logiciel. Le modèle d'octroi de licences devrait être présenté afin d'obtenir des points pour ce critère.

C. Le soumissionnaire devrait remplir le tableau suivant en mettant un X dans la colonne appropriée, afin d'indiquer si l'exigence sera remplie par la technologie de portail Web proposée en réponse au critère O3, en cochant « prêt à l'emploi » ou « besoin de configuration »… »

Réponse nº 221 :

Les critères d'évaluation O3 et C10 ont été supprimés de l'évaluation technique. Veuillez consulter la réponse à la question n° 210 de la présente modification pour en savoir plus.

Question nº 222 :

Compte tenu des restrictions apportées à modification 008, réponse 110 ("En outre, aucun lien électronique ne sera fourni entre les systèmes du gouvernement du Canada et Contractors TI") si les fournisseurs supposent que, pour accéder à une instance GC IBM Pure Data warehouse correctement configurée, pour non-production utilise, les ressources du fournisseur doivent être mises sur le site pour accéder (cette question est posée afin que tous les fournisseurs soient évalués également compte tenu de la nouvelle restriction)?

Réponse nº 222 :

L'État confirme que tous les travaux liés au projet dans le cadre desquels une personne doit avoir un accès direct aux renseignements et aux biens protégés du gouvernement du Canada devront être effectués sur place. Comme indiqué, dans le cadre de l'entrepôt de données pures IBM du gouvernement du Canada, l'entrepreneur devra se trouver sur place.

Veuillez vous reporter à la réponse à la question nº 219 de la présente modification.

Question nº 223 :

Étant donné que :

a) bon nombre de nos questions sont toujours sans réponse;

b) la date limite pour soumettre des questions était le 5 septembre;

c) le secteur d'activité ne disposera pas encore d'assez de temps pour modifier de façon appropriée les propositions en réponse aux changements apportés par l'État qui figureront dans les nouvelles modifications, ni pour demander des précisions sur ces changements;

nous demandons respectueusement à l'État de repousser la date de clôture de la demande de propositions au 30 septembre 2017.

Réponse nº 223 :

La date de clôture des soumissions est reportée au 2 octobre 2017.

TOUTES LES AUTRES MODALITÉS DEMEURENT INCHANGÉES.

ANNEXE A – ÉNONCÉ DES TRAVAUX

TABLE DES MATIÈRES

LISTE DES ANNEXES

PARTIE 1 : APERÇU DE LA SOLUTION DE SÉCURITÉ INDUSTRIELLE DU CANADA

Le portefeuille d'applications opérationnelles qui appuie la prestation des services de sécurité industrielle est en grande partie désuet et non viable. Cette lacune nuit aux efforts déployés par le Secteur de la sécurité industrielle (SSI) pour répondre aux attentes de ses utilisateurs et de ses partenaires de l'industrie et du gouvernement. Pour régler ce problème, le SSI envisage de moderniser la plateforme technologique qui soutient ses opérations.

Les sections suivantes donnent le contexte du projet en cours et des renseignements généraux sur celui-ci et tentent de déterminer clairement les contraintes, les hypothèses et les attentes.

1.1 CONTEXTE

1.1.1 Programme de sécurité industrielle

Travaux publics et Services gouvernementaux Canada (TPSGC) est reconnu comme l'un des dix principaux organismes responsables de la sécurité du gouvernement du Canada (GC). Au moyen de son leadership et de ses activités de coordination, TPSGC veille à l'application des mesures de sécurité à toutes les étapes du processus de passation des marchés qui relèvent du Programme de sécurité industrielle (PSI).

TPSGC est tenu d'offrir les services du PSI, notamment :

(a) élaborer, en fonction d'une analyse des besoins de la collectivité et en collaboration avec le Secrétariat du Conseil du Trésor (SCT), des instruments de politique, des lignes directrices et des outils dans le domaine de la sécurité des marchés aux fins d'approbation par le SCT;
(b) coordonner l'élaboration et la présentation de séances de formation et de sensibilisation à la sécurité dans la passation des marchés;
(c) diriger des groupes de travail et des comités interministériels responsables de la sécurité des marchés pour faciliter l'échange de renseignements et la collaboration entre les collectivités de pratique;
(d) recenser et examiner les pratiques de sécurité dans la passation des marchés et formuler des recommandations à l'intention du SCT et des comités de gouvernance de la sécurité afin de favoriser l'amélioration des politiques de sécurité et la collaboration entre les ministères;
(e) tenir à jour une base de données des organisations du secteur privé et des personnes qui ont obtenu l'autorisation d'accéder à des renseignements et à des biens classifiés et protégés;
(f) remplir divers rôles découlant des accords internationaux en matière de sécurité industrielle;
(g) mener des inspections des entreprises qui ont accès aux renseignements et aux biens protégés et classifiés des alliés de l'OTAN ou des entreprises qui sont enregistrées auprès des pays avec lesquels le Canada a conclu un protocole d'entente en matière de sécurité industrielle;
(h) traiter les demandes de visite lorsqu'une personne ayant une autorisation de sécurité doit visiter une organisation gouvernementale ou commerciale au Canada ou à l'étranger;
(i) effectuer les enquêtes de sécurité nécessaires à l'égard des personnes et des organisations du secteur privé qui ont accès à des renseignements et à des biens protégés et classifiés, y compris celles qui participent à des marchés avec l'étranger;
(j) vérifier la conformité des marchés liés à la sécurité qui donnent accès à des renseignements et à des biens du gouvernement;
(k) contrôler et gérer les biens de sécurité des communications (SECOM) pour les entreprises du secteur privé et effectuer les enquêtes de sécurité et les inspections à l'égard des biens SECOM pour les entreprises du secteur privé;
(l) représenter le gouvernement du Canada dans le cadre d'initiatives nationales et internationales liées à la sécurité des marchés et aux marchandises contrôlées.

Le PSI est offert par le Secteur de la sécurité industrielle (SSI) de la Direction générale de la surveillance (DGS) de TPSGC.

Le SSI offre deux programmes : le Programme de sécurité des contrats (PSC) et le Programme des marchandises contrôlées (PMC). Voir l'appendice 1 de l'annexe A pour plus de renseignements sur les processus opérationnels propres aux programmes.

1.1.1.1 Programme de sécurité des contrats

Le PSC du GC offre des services qui sont essentiels pour les Canadiens et les Canadiennes et pour la protection des renseignements et des biens qui sont confiés à des organisations canadiennes et internationales du secteur privé et à leurs gouvernements. Le programme permet d'une part au GC de confier des technologies secrètes canadiennes et étrangères à l'industrie canadienne et d'autre part à l'industrie canadienne de participer à des contrats à l'étranger de nature classifiée. Le programme permet de garder la confiance de l'OTAN et des autres alliés du Canada et il appuie les priorités du Canada en matière d'anti-prolifération, de sécurité publique, de sécurité et de sécurité mondiale.

Les fonctions propres au PSC en matière de sécurité des contrats comprennent :

(a) fournir des services de filtrage de sécurité du personnel et des installations aux organisations du secteur privé canadien qui participent à des marchés publics protégés ou classifiés;
(b) inspecter les organisations ayant accès à des biens ou à des renseignements protégés et classifiés;
(c) traiter les demandes des visiteurs canadiens et étrangers devant avoir accès à des biens ou des renseignements classifiés ou protégés liés au programme ou à des marchés;
(d) transmettre les biens ou les renseignements classifiés ou protégés liés au programme ou à des marchés entre les industries et les gouvernements du Canada et des autres pays.

Le PSC est actuellement opérationnel et il engage approximativement 396 employés, tous regroupés à Ottawa.

1.1.1.2 Programme des marchandises contrôlées

Le PMC est un programme d'inscription et de conformité qui régit l'accès aux marchandises contrôlées au Canada, y compris celles visées par l'*International Traffic in Arms Regulations* (ITAR). Le PMC joue un rôle important dans la prévention et la détection de l'examen, de la possession et du transfert non autorisés de marchandises contrôlées au Canada. Conformément à la *Loi sur la production de défense* et au *Règlement sur les marchandises contrôlées*, le mandat du PMC consiste à renforcer les contrôles canadiens en matière de commerce de défense au moyen de processus d'inscription et de réglementation obligatoires des entreprises et des personnes qui doivent examiner des marchandises contrôlées ou en prendre possession ou les transférer.

Le PMC est responsable de la réglementation pour environ 4 000 entreprises canadiennes susceptibles d'examiner, de posséder et de transférer des marchandises contrôlées. Le programme est appliqué en collaboration étroite avec les partenaires responsables de la sécurité nationale (le Service canadien du renseignement de sécurité, la Gendarmerie royale du Canada, l'Agence des services frontaliers du Canada et Affaires mondiales Canada) dans le but de procéder à des évaluations de sécurité pour les personnes ou les entreprises, d'évaluer les risques pour la sécurité, d'offrir une formation aux représentants désignés des entreprises inscrites, de mener des enquêtes et d'appliquer les mesures de conformité.

Le PMC est actuellement opérationnel et il engage approximativement 91 employés, tous regroupés à Ottawa.

1.1.2 Projet de transformation des systèmes de sécurité industrielle

Besoins opérationnels

Le SSI doit remplacer son groupe de systèmes existant utilisé pour la sécurité des contrats et le contrôle des marchandises par une solution stable, évolutive et conviviale qui s'intègre parfaitement. Il est essentiel de tenir compte des écarts en matière d'expérience, de capacité, de rendement et de conformité que l'on peut observer actuellement entre les systèmes actuels du SSI et les attentes de l'industrie et du GC, notamment les problèmes touchant le rendement et la stabilité des systèmes, le risque d'erreur et le traitement manuel intensif des dossiers. Tout cela a des répercussions sur le maintien des normes de service du SSI dans certains domaines, ce qui en retour a une incidence sur l'attribution des contrats et, par le fait même, sur les revenus de l'industrie. Le SSI doit faciliter l'expérience de l'utilisateur auprès du GC et ses interactions avec celui-ci de manière à respecter les objectifs de modernisation du gouvernement tout en préservant les paramètres de sécurité appropriés.

1.1.2.1 Objectifs du projet

L'étendue et l'objectif du projet de transformation des systèmes de sécurité industrielle (TSSI) consistent à remplacer l'ancien groupe de systèmes existant qui soutient les fonctions du PSC et du PMC au sein du SSI par une solution unique qui gère mieux les besoins actuels et émergents de l'industrie et du GC. Dans le cadre du projet du TSSI, le processus de réorganisation des processus opérationnels est nécessaire afin d'harmoniser les activités du SSI et la solution proposée.

1.1.2.2 Résultats attendus

Les exigences en matière d'évolutivité, de capacité soutenue, de sécurité et de stabilité sont devenues des facteurs essentiels à la capacité de TPSGC d'offrir des services essentiels pour le compte du GC. L'intégration des processus et des solutions, les gains d'efficacité accrus et une plus grande harmonisation avec les fonctions actuelles des programmes permettront au SSI de satisfaire et de surpasser les normes de service et d'assurer la communication des renseignements et la surveillance de manière plus efficace.

La solution consiste à fournir aux utilisateurs du GC et à l'industrie une interface électronique libre-service conviviale de communication avec le SSI. À l'interne, on s'attend à ce que le système permette au SSI de gérer des flux de travaux automatisés et configurables qui entraîneront des gains d'efficacité dans le but de respecter les normes de rendement et de dépasser de beaucoup les niveaux de rendement actuels, dont le SSI s'attend à être amélioré. Voici quelques exemples de normes établies :

(a) Vérification d'organisation désignée – jusqu'à six mois après la réception de la demande dûment remplie;
(b) Attestation de sécurité de l'installation – six mois ou plus après la réception de la demande dûment remplie et selon la complexité du filtrage exigé;
(c) Cote de fiabilité pour une demande simple – dans un délai de sept jours ouvrables suivant la réception de la demande dûment remplie;
(d) Cote de fiabilité pour une demande complexe – dans un délai de 120 jours ouvrables suivant la réception de la demande dûment remplie;
(e) Demande d'attestation de sécurité de niveau « Secret » – dans un délai de 75 jours ouvrables (en plus du délai pour la vérification de la fiabilité) suivant la réception de la demande dûment remplie;
(f) Demande d'inscription au PMC – dans un délai de 45 jours suivant la réception de la demande dûment remplie.

Une mise en œuvre complète de ce système nous permettra d'obtenir un certain nombre de résultats opérationnels avantageux et mesurables, principalement les suivants :

(a) capacité accrue (p. ex., pour inscrire les entreprises et traiter les autorisations de sécurité et les demandes d'inscription);

(b) service amélioré (p. ex., un processus de demande et d'autorisation de sécurité plus fiable et plus rapide);
(c) communication de renseignements améliorée (p. ex., capacité complète de recherche et de production de rapports);
(d) satisfaction accrue (p. ex., des processus conviviaux et simplifiés axés sur l'utilisateur pour l'industrie et les autres utilisateurs);
(e) gains d'efficacité supérieurs (p. ex., réduction des coûts liés à la conformité des fournisseurs).

Voici quelques autres exemples d'avantages ou de résultats positifs :

Assurer la sécurité et la protection des renseignements personnels et des biens d'origine canadienne	
Sécurité	• Réduction des violations relatives à la sécurité ou à la confidentialité
Obtenir un meilleur rapport qualité-prix pour les utilisateurs et l'industrie	
Outils de libre-service	• Réduction des plaintes de l'industrie
	• Réduction du nombre de formulaires incomplets reçus
	• Réduction du nombre de demandes de renseignements
Simplification de la prestation de services et réduction du fardeau administratif	• Réduction des délais de traitement des demandes
	• Réduction des délais requis pour répondre aux questions ou préoccupations (problèmes liés au traitement des demandes, requêtes de suivi des clients)
	• Partage des données de base entre les différents secteurs d'activité du SSI
Gouvernement innovateur et efficient	
Optimisation des ressources	• Réduction des coûts administratifs (p. ex. la manutention, la conservation ou l'élimination de documents)
Innovation	• Plus grande automatisation des processus de travail
	• Élimination de la nécessité d'avoir des signatures manuscrites
	• Intégration aux solutions existantes du GC
Gestion efficace de l'information	• Production de rapports améliorée et uniforme
	• Réduction du nombre d'étapes des processus de travail
	• Réduction du nombre d'étapes manuelles au sein des processus de travail

2.1 NOUVELLE SOLUTION

Le diagramme suivant illustre la carte d'interaction de haut niveau pour la solution TSSI requise. Illustrés sont les types d'utilisateurs de haut niveau utilisant le service d'authentification cybernétique GCpour accéder au services

vertical web initial destinées au public de la solution TSSI afin de soumettre des demandes de service à l'application de traitement des services de la solution TSSI. Veuillez vous référer à http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26262 pour plus d'informations sur le service d'authentification cybernétique GC. Alternativement, les utilisateurs peuvent remplir des formulaires qui rempliront les codes à barres intégrés avec des informations sur les formulaires, puis soumettront ces demandes de service pour traitement. Les formulaires reçus seront numérisés à l'aide d'un code à barres afin de saisir les informations de formulaires dans l'application de traitement des services de la solution TSSI.

L'application de traitement des services de la solution TSSI sera utilisée pour traiter les demandes de service soumises avec des interfaces gouvernementales externes et internes. Par exemple, la solution de l' TSSI interagira avec la Gendarmerie royale du Canada (GRC) pour effectuer des vérifications des antécédents judiciaires pour les demandes de services de contrôle de sécurité du personnel. La solution TSSI maintiendra un dépôt de documents, permettra l'accès à distance aux inspecteurs et aux enquêteurs du PSC et du DCM.

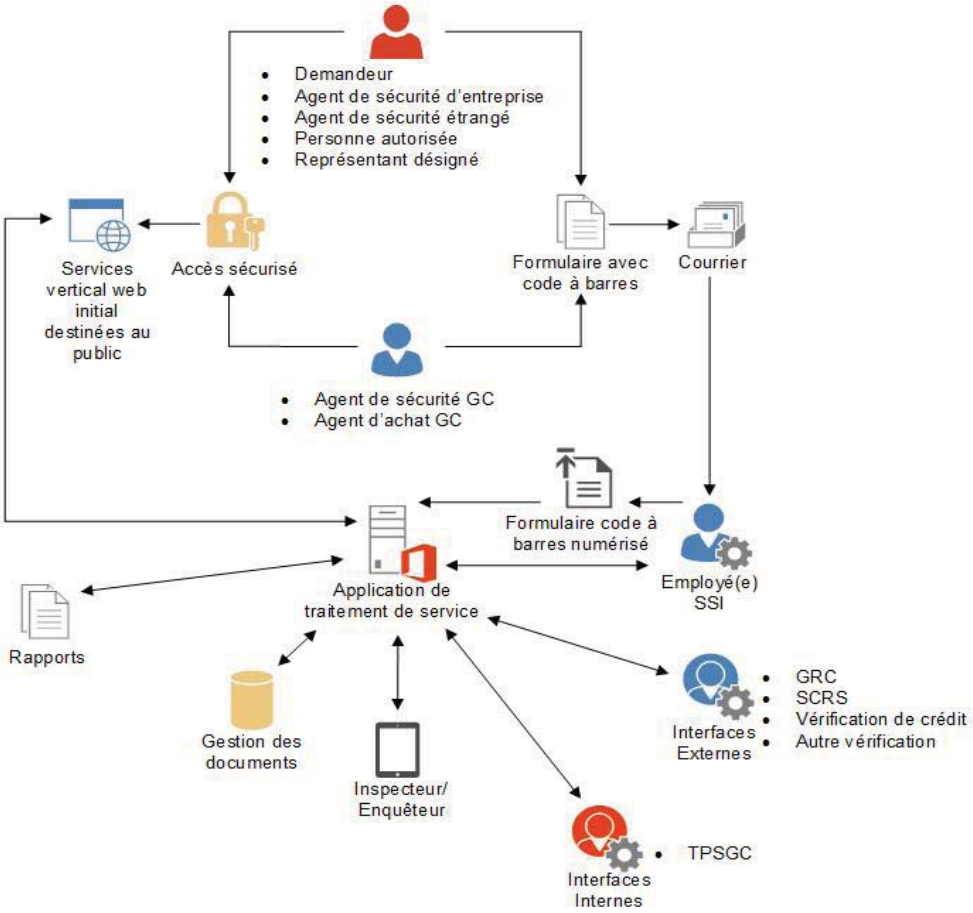


Figure 1: Carte d'interaction de haut niveau de la solution ISST.

3.1 DONNÉES VOLUMÉTRIQUES

Les données volumétriques ci-dessous décrivent les volumes que la solution proposée devrait prendre en charge, selon les attentes.

3.1.1 Comptes d'utilisateurs

Comptes d'utilisateurs internes : Actuellement, il y a 487 comptes d'utilisateurs au total, dont 396 pour le

PSC et 91 pour le PMC. Comptes d'utilisateurs externes : Actuellement, il y a 183 905 comptes d'utilisateurs au total, répartis comme suit :

(a) utilisateurs externes pour le PSC – industrie : 161 000 comptes d'utilisateurs;
(b) utilisateurs externes pour le PSC – gouvernement : 905 comptes d'utilisateurs;
(c) utilisateurs externes pour le PMC – 22 000* comptes d'utilisateurs.

3.1.2 *Remarque : Actuellement, il n'y a pas de comptes d'utilisateurs externes pour le PMC. Cependant, on estime que la solution facilitera l'accès pour un nombre approximatif de 22 000 comptes d'utilisateurs externes du PMC. Volumes par activité

Voici les différentes transactions relatives aux activités du SSI, accompagnées des volumes annuels et quotidiens. Les volumes rapportés sont fondés sur les totaux de l'exercice 2015-2016.**Inscription au PSC et au PMC**

Le PSC offre des services d'inscription aux organisations canadiennes qui remplissent des contrats du GC comportant des exigences de sécurité. Actuellement, plus de 18 400 organisations canadiennes sont inscrites au PSC.

L'inscription au PMC est obligatoire en vertu de la loi pour toute personne (personne physique ou morale) qui examine, possède ou transfère des marchandises contrôlées au Canada. Actuellement, plus de 4 500 Canadiens et Canadiennes et entreprises canadiennes sont inscrits au PMC.

Vous trouverez ci-dessous le sommaire des activités liées à l'inscription au PSC ou au PMC :

Sommaire des activités liées à l'inscription	**PSC**		**PMC**		**Total**	
	Annuelles	**Quotidiennes**	**Annuelles**	**Quotidiennes**	**Annuelles**	**Quotidiennes**
Nouvelles inscriptions	3 438	13	454	2	3 892	15
Renouvellements d'inscriptions	2 889	11	514	2	3 403	13
Modifications d'inscriptions	337	1	352	1	689	2
Résiliations d'inscriptions	3 124	12	306	1	3 430	13
Inspections et enquêtes	5 342	20	1 804	7	7 146	27
Total des activités liées à l'inscription	**15 130**	**57**	**3 430**	**13**	**18 560**	**70**

Demandes de filtrage de sécurité du personnel ou d'autorisation de sécurité pour des membres du personnel

Le personnel d'une organisation inscrite au PSC qui exécute un contrat assorti d'exigences en matière de sécurité doit passer par un contrôle de sécurité et obtenir une autorisation de sécurité avant d'avoir accès à des emplacements, à des ressources ou à des renseignements protégés ou classifiés. Le PSC offre un service de filtrage de sécurité du personnel et d'autorisation de sécurité à l'égard du personnel aux autres organisations du GC.

Actuellement, le PSC gère approximativement **850 000** dossiers de filtrage de sécurité du personnel et d'autorisation de sécurité.

Vous trouverez ci-dessous le sommaire des demandes de sécurité faites pour des membres du personnel dans le cadre du PSC :

Activités de filtrage de sécurité du personnel ou d'autorisation de sécurité pour des membres du personnel		
	Annuelles	Quotidiennes
Demandes de vérification aux fins d'une cote de fiabilité	86 907	333
Demandes d'autorisation de sécurité	42 772	164
Demandes liées à une cessation d'emploi	42 783	162
Fermetures	17 163	66
Demandes d'évaluation de sécurité pour le PMC	1 194	6
Total des activités relatives au filtrage de sécurité du personnel ou aux autorisations de sécurité pour des membres du personnel	**190 819**	**731**

Demandes relatives à la sécurité des contrats

Le PSC fournit des clauses de sécurité aux autorités contractantes pour les contrats du gouvernement, en fonction des exigences de ces contrats en matière de sécurité. Pour l'exercice financier 2015-2016, le PSC a reçu 10 250 demandes de service (39 par jour) préalables à l'attribution de contrats (Liste de vérification des exigences relatives à la sécurité) et 9 062 demandes de service (35 par jour) liées aux contrats déjà attribués (p. ex., les contrats de sous-traitance ou les modifications de contrats).

PSC – Demandes de visite

Les demandes de visite présentées dans le cadre du PSC sont requises lorsqu'une personne doit faire affaire avec une organisation du gouvernement ou du secteur privé au Canada ou à l'étranger en vue d'avoir accès à des biens ou des renseignements à caractère sensible dans le cadre d'un contrat gouvernemental. Pour l'exercice financier 2015-2016, le PSC a enregistré 6 617 demandes de service (25 par jour) pour des visites.

PSC – Demande de contrôle des documents

Les renseignements, les biens et le matériel protégés ou classifiés doivent être transférés par les circuits officiels lorsqu'ils entrent au Canada ou lorsqu'ils quittent le pays. Pour l'exercice financier 2015-2016, le PSC a traité 226 demandes de contrôle des documents (1 par jour).

PMC – Demandes d'exemption pour un visiteur

Les demandes d'exemption pour un visiteur faites dans le cadre du PMC concernent les personnes qui visitent une organisation inscrite au PMC et qui ne sont pas tenues de faire l'objet d'une évaluation de sécurité. Pour l'exercice financier 2015-2016, le PMC a enregistré 1 352 demandes d'exemption pour visiteurs (5 par jour).

PMC – Demandes d'exemption pour un travailleur temporaire

Les demandes d'exemption pour un travailleur temporaire faites dans le cadre du PMC concernent les personnes qui occuperont un poste temporaire dans une organisation inscrite au PMC et qui ne sont pas tenues de s'inscrire

elles-mêmes au PMC. Pour l'exercice financier 2015-2016, le PMC a reçu 299 demandes d'exemption pour travailleurs temporaires (1 par jour).

PMC – Demandes de recommandation visant un employé

Les recommandations visent les employés posant un risque jugé être de niveau modéré ou élevé. Pour l'exercice financier 2015-2016, le PMC a reçu 23 demandes de recommandation.

PSC et PMC – Volume d'appels au centre d'appels

Demandes de renseignements effectuées auprès du centre d'appels du PSC et du PMC. Pour l'exercice financier 2015-2016, le centre d'appels a reçu 124 970 demandes de vérification (479 par jour) relatives à la sécurité du personnel et à l'organisation et 110 331 demandes de renseignements (423 par jour).

Volume des documents justificatifs

Les estimations du volume des pages sont fondées sur un vaste éventail de demandes, allant des demandes habituelles aux demandes pour des situations extrêmes. Afin d'extrapoler une taille sur la base de ces données, on a utilisé un facteur de multiplication de 11 Ko (représentant une page d'un seul mot) ainsi que les totaux pour l'exercice financier 2015-2016 et une estimation du volume quotidien.

Secteur d'activité	Programme	Nombre de pages min.	Nombre de pages max.	Total pour 2015-2016	Volume min. pour 2015-2016 (Go)	Volume max. pour 2015-2016 (Go)	Total quotidien pour 2015-2016	Volume min. quotidien pour 2015-2016 (Go)	2015-2016 Volume quotidien max. (Go)
Marchés	PSC	20	500	19 312	4,1	101,3	74	0,016	0,397
Inscription[1]	PSC	100	1 000	9 788	10,3	102,7	38	0,041	0,408
	PMC	60	100	1 626	1,0	1,7	6	0,004	0,006
Inspection et enquête[2]	PSC	100	1 500	15 865	16,6	249,6	61	0,066	0,983
	PMC	30	100	1 804	0,6	1,9	7	0,002	0,008
Sécurité du personnel[3]	PSC	10	100	189 625	19,9	198,9	727	0,078	0,781
	PMC	20	50	1 194	0,3	0,6	5	0,001	0,003
Visites	PSC	20	50	6 617	1,4	3,5	25	0,005	0,013
	PMC	9	15	1 352	0,1	0,2	5	0,000	0,001
Exemptions pour un travailleur temporaire et recommandations visant un employé	PMC	20	30	322	0,1	0,1	1	0,0002	0,0003
Contrôle des documents	PSC	20	50	226	0,1	0,1	1	0,0002	0,0005

[1] Total des activités liées à l'inscription (nouvelle inscription, renouvellement, modification et résiliation).

[2] Cela comprend les activités d'inspection et d'enquête aux fins d'obtention d'une autorisation de sécurité pour une organisation ou un membre du personnel.
[3] Total des activités de sécurité liées à un nouveau membre du personnel ou à une cessation d'emploi.

4.1 TERMINOLOGIE COMMUNE

Les principaux termes et sigles utilisés partout dans le présent document sont définis à l'appendice 6 de la présente ANNEXE.

PARTIE 2 : EXIGENCES OPÉRATIONELLES

La présente section décrit les exigences de restructuration des processus opérationnels et les exigences fonctionnelles pour la solution.

1.1 APERÇU DES EXIGENCES – RESTRUCTURATION DES PROCESSUS OPÉRATIONNELS

Le lancement d'un nouveau système est l'occasion idéale de passer en revue, rationaliser, simplifier et améliorer la prestation des services du Secteur de la sécurité industrielle. Une analyse rigoureuse des procédures et des processus existants est nécessaire pour proposer des processus regroupés plus simples et plus rapides qui procurent des gains d'efficacité concrets et mesurables.

Le SSI exige l'élaboration et la réalisation d'une stratégie de restructuration des processus opérationnels qui produira des avantages mesurables en fonction de chacun des critères ci-dessous tout en améliorant les niveaux de service à l'industrie :

(a) réduction des étapes du processus;
(b) réduction des formalités administratives;
(c) réduction des étapes manuelles;
(d) réduction des délais de traitement;
(e) automatisation maximale des processus.

Les mesures de rendement étudiées comprennent la qualité et l'efficacité des services fournis.

Dans plusieurs cas, les processus du SSI sont présentement fortement basés sur le papier. De même, les processus du SSI requièrent une bonne part de traitement manuel. Dans la mesure du possible, il faut remplacer les processus manuels par les fonctions prises en charge par le système et réduire considérablement, voire éliminer totalement, la nécessité des processus qui dépendent de formulaires papier.

On pourrait automatiser complètement certains processus. Dans ce contexte, « automatiser complètement » veut dire un processus qui reçoit la demande et réalise le processus subséquent en entier, sans aucune intervention humaine. L'un de ces processus est le processus de vérification de la fiabilité pour la sécurité du personnel. On s'attend à ce que l'automatisation complète des vérifications de fiabilité (simples) fasse partie de la stratégie et de la solution proposées par l'entrepreneur. Tous les autres processus pourraient être des candidats viables à une automatisation complète ou partielle. Consultez l'appendice 1 de l'annexe A pour obtenir plus de renseignements par rapport aux processus clés de SSI inclu23ant la vérification de la fiabilité.

Une restructurationefficace des processus opérationnels a pour but de :

(a) repenser complètement les processus opérationnels;
(b) simplifier, consolider et remanier les processus opérationnels;
(c) optimiser les processus de bout en bout et automatiser les tâches;
(d) supprimer, remplacer ou regrouper les processus qui n'ajoutent pas de valeur opérationnelle;
(e) répondre aux attentes des intervenants sur le plan de l'innovation, de l'adaptation aux besoins, de la rapidité, de la qualité et du service.

L'entrepreneur doit s'assurer que la coordination de la restructuration des processus opérationnels est en ligne avec le plan, les activities et toutes autres activitiés reliées au plan de gestion du project et le calendrier du projet.

1.2 EXIGENCES DÉTAILLÉES – RESTRUCTURATION DES PROCESSUS OPÉRATIONNELS

L'entrepreneur doit:

Catégorie	Section de l'EDT	Exigence
Restructuration des processus opérationnels	BR.01	Préparer un plan de restructuration des processus opérationnels qui inclut mais n'est pas limité à : (a) L'élaboration des objectifs pour la restructuration des processus opérationnels en ce qui concerne la solutionTSSI; (b) L'objectif stratégique de la restructuration des processus opérationnels dans le cadre de la solution de l'TSSI; (c) Elaborer sur la façon dont l'analyse des écarts de restructuration des processus opérationnels sera menée; (d) Élaborer sur la manière dont les contraintes et les impacts seront pris en compte en conséquence de la restructuration des processus de gestion; et (e) Fournir des détails sur la planification des activités de restructuration des processus de gestion.
	BR.02	Effectuer une analyse détaillée des processus opérationnels actuels, de formulaires de demande de service, des flux de travaux et des règles opérationnelles correspondantes.
	BR.03	Développer une proposition de restructuration des processus opérationnels qui décrit les modèles de processus proposés, souligne les changements majeurs ainsi que les processus qui ajoutent de la valeur et les résultats attendus.
	BR.04	Concevoir les futurs processus, flux de travaux, fonctions de solution et développer les schémas de processus opérationnels.
	BR.05	Créer, les cas échéants, des nouveaux formulaires de demande de service inclus dans la solution afin de faciliter la saisie électronique de l'information requise pour le processus. Par exemple, il n'existe actuellement aucun formulaire de demande de service pour l'enregistrement d'une organisation avec le PSC.
	BR.06	Dans la mesure du possible, proposer et modifier des formulaires de demande de service existants pour faciliter la saisie et le traitement de la demande. Par exemple, les formulaires d'inscription PMC peuvent être mis à jour si nécessaire. Veuillez noter que les formulaires utilisés pour le dépistage des autorisations de sécurité du personnel sont élaborés par le SCT et pourront possiblement pas être disponibles pour modification.
	BR.07	Effectuer une analyse d'écart pour identifier les secteurs (les processus de gestion et les utilisateurs à la suite de la restructuration des processus) pour l'engagement futur dans la gestion du changement.

Catégorie	Section de l'EDT	Exigence
	BR.08	Déterminer les mesures appropriées pour identifier le succès et élaborer des critères de mesure de rendement qui seront utilisés plus tard dans le cadre de l'évaluation de l'état de préparation opérationnelle.
	BR.09	Developper l'architecture d'entreprise pour la solution.
	BR.10	Effectuer une analyse simulée des options pour déterminer les améliorations optimales.
	BR.11	Démontrer la réussite de la restructuration des processus opérationnels en exécutant un processus identifié du début à la fin qui touche toutes les fonctionnalités principales identifiées par les exigences dans les besoins opérationnels détaillés de l'annexe A (section 2 de l'annexe A). Le processus identifié sera choisi par l'entrepreneur après avoir complété l'analyse des écarts et la restructuration des processus opérationnels.
	BR.12	Intégrer et mettre en œuvre des processus et des flux de travail qui seront approuvés dans la conception de la solution.
	BR.13	Les risques identifiés lors de la restructuration des processus métiers doivent être intégrés dans le registre des risques du projet (annexe A, section 7).
	BR.14	Fournir des recommandations sur les meilleures actions à prendre pour traiter et résoudre les problèmes des intervenants.
	BR.15	Fournir un rapport d'étape et un registre de risques à chaque mois.
	BR.16	Élaborer des procédures opérationnelles standardisées de début à fin axées sur les processus qui décrivent les activités principales et la responsabilité des utilisateurs afin que les utilisateurs ultimes soient informés de la façon dont la restructuration des processus d'entreprise affecte leurs activités quotidiennes.
	BR.17	Coordonner les activités de restructuration des processus opérationnels aux activités de gestion du changement nécessaires pour faciliter une adoption de la solution.
	BR.18	Fournir un rapport de restructuration des processus opérationnels décrivant l'ensemble des démarches entreprises, les résultats d'analyse, la nouvelle conception, les gains d'efficacité et les avantages prévus, les critères d'évaluation à utiliser, les liens avec le plan de gestion du changement et les leçons apprises. Le rapport de restructuration des processus opérationnels nécessite la révision et l'approbation par l'autorité responsable du projet.
	BR.19	Préparer une stratégie préliminaire de restructuration des processus opérationnels qui comprend, sans toutefois s'y limiter : (a) la compréhension des processus opérationnels actuels du Secteur de la sécurité industrielle (SSI) et de la nécessité de recourir à des pratiques en matière de sécurité dans le cadre des diverses activités opérationnelles; (b) un plan pour effectuer une analyse des écarts des processus opérationnels;

Catégorie	Section de l'EDT	Exigence
		(c) la compréhension des contraintes et des répercussions; (d) quatre exemples d'occasions d'accroître l'efficience et l'efficacité et la rentabilité des processus et les méthodes de mise en œuvre proposées; (e) la compréhension des risques et des possibilités aux fins d'atténuation et de résolution des risques; la planification des activités de restructuration des processus opérationnels.
	BR.20	Préparer une stratégie de restructuration des processus opérationnels après que la stratégie préliminaire de restructuration des processus opérationnels ait été évaluée par le Canada et que l'on ait jugé que la stratégie satisfait aux exigences et aux avantages énumérés ci-dessus.

2.1 SOMMAIRE DES EXIGENCES – EXIGENCES FONCTIONELLES

La solution est une application opérationnelle qui comprend deux volets majeurs : une application de traitement du service et un service vertical web initial destinées au public

L'application de traitement du service est le volet de la solution qui prend en charge le traitement des demandes de service du Secteur de la sécurité industrielle en fournissant, entre autres, les résultats suivants :

(a) soutenir la réalisation de gains d'efficacité opérationnelle supérieurs au moyen de la simplification et de l'automatisation complète ou partielle des processus opérationnels du SSI;
(b) offrir une interface conviviale qui favorise un traitement efficace du service;
(c) permettre aux utilisateurs internes de communiquer efficacement avec les utilisateurs et entités externes;
(d) permettre aux utilisateurs internes de gérer efficacement un dossier pendant la totalité de son cycle de vie;
(e) soutenir et maintenir des données de haute qualité relatives aux dossiers ainsi que leurs relations;
(f) soutenir des mécanismes de validation intégrés visant à vérifier le caractère complet et exact des données et des processus;
(g) soutenir le programme écologique du GC en remplaçant les flux de travaux et les processus sur papier;
(h) soutenir l'accès à distance aux dossiers;
(i) permettre l'acquisition, l'entreposage et la communication de renseignements à l'appui (documents justificatifs et correspondance connexe) au format électronique;
(j) interagir avec d'autres applications du GC et permettre l'interconnectabilité avec des organismes externes;
(k) Facilite le reportage sur les activités opérationnelles et les tendances du SSI grâce à des rapports disponibles; et;
(l) une solution qui met en œuvre les services de base offerts par le SSI;

Le service vertical web initial destinées au public est le volet d'échange de données sur Internet de la solution qui est utilisé par le public et qui sert d'interface libre-service centrale et habilitante permettant les communications et les interactions entre les utilisateurs externes et les deux programmes du Secteur de la sécurité industrielle : le Programme de sécurité des contrats et le Programme des marchandises contrôlées. Les résultats attendus pour le service vertical web initial destinées au public comprennent notamment : offrir un point d'accès unique sécuritaire aux services du SSI;

(a) permettre aux utilisateurs externes de gérer de façon autonome des aspects de leurs demandes de service et de leurs profils;
(b) permettre aux utilisateurs externes de gérer eux-mêmes les aspects de leurs demandes de service et de leurs profils;
(c) permettre aux utilisateurs externes de configurer leur portefeuille de services libre-service en fonction de leurs préférences (p. ex., leurs favoris);
(d) permettre aux utilisateurs externes d'avoir accès aux services du SSI sans qu'il leur soit nécessaire d'avoir des interactions directes avec un représentant du SSI ni de suivre une formation particulière;
(e) offrir aux utilisateurs externes un point de communication unique avec le SSI pour leur permettre d'avoir accès à des renseignements généraux et d'échanger avec le SSI des renseignements liés à leurs demandes de service de façon efficace, sécuritaire et rapide;
(f) offrir aux utilisateurs externes une mobilité ou une accessibilité améliorée;
(g) offrir aux utilisateurs externes un autre moyen de présenter les demandes au SSI;
(h) permettre d'augmenter la base d'utilisateurs de la solution par différents ordres de grandeur sans réduire le niveau de service fourni;
(i) offrir une acquisition des données très fidèle;
(j) permettre de répondre à la transaction de l'utilisateur externe presque en temps réel.

Une composante du passage des systèmes actuels hérités à la nouvelle solution sera la migration des données identifiées. La planification, le développement et la validation de la migration de données doivent être remplis par l'entrepreneur en utilisant une taille d'échantillon contrôlée des données qui couvre les divers types de données et les éléments présentement entreposés. Bien que l'entrepreneur devra planifier la migration des données, l'entrepreneur ne devra pas effectuer la migration des données réelles. On s'attend à ce que TPSGC BDPRH/SPC effectue la migration des données en suivant la stratégie et le plan de migration de données élaborés par l'entrepreneur.

2.2 EXITENCES DÉTAILLÉES – EXIGENCES FONCTIONNELLES

2.2.1 Application de traitement du service

L'entrepreneur doit livrer une application de traitement du service qui comporte, sans s'y limiter, les fonctions suivantes :

Catégorie	Section de l'EDT	Exigence
Automatisation	APP-AU.01	Automatisation, en tout ou en partie, des processus opérationnels du SSI. Par exemple, l'automatisation des demandes simples d'autorisation de sécurité aux fins de vérification de la fiabilité du personnel et de duplication d'autorisations quand tous les critères de validation de la demande sont satisfaits lors de la soumission de la demande par l'utilisateur externe. Voir l'appendice 1 de l'annexe A pour obtenir plus de détails sur les processus simples de duplication ou de vérification de la fiabilité.
	APP-AU.02	Émission automatique des certificats d'approbation appropriés (par exemple, le Certificat d'enquête de sécurité et profil de sécurité) : (a) Pour les demandes de service qui respectent tous les critères obligatoires désignés (par exemple, la vérification des partenaires de sécurité); (b) Envoi d'un avis à l'utilisateur externe indiquant que sa demande de service a été approuvée; (c) Production du certificat d'approbation approprié comprenant les signatures et les dates de validation correspondantes de la demande; (d) Accessibilité au certificat d'approbation approprié par l'utilisateur externe aux fins de téléchargement et d'impression à partir du service vertical web initial destinées au public.
	APP-AU.03	Gestion automatique des comptes d'utilisateurs : (a) Elle crée automatiquement des comptes temporaires pour les utilisateurs externes de type « demandeur » à la demande d'un utilisateur externe de type « agent de sécurité » ou « représentant désigné », conjointement avec l'exigence *WP-UE.01*; (b) Elle désactive automatiquement les comptes temporaires pour les utilisateurs externes de type « demandeur » une fois que la demande de filtrage de sécurité du personnel connexe est terminée ou après une période d'inactivité prédéterminée; (c) Elle désactive automatiquement les comptes qui appartiennent aux organisations qui ne sont plus inscrites (ou dont l'inscription a été résiliée) auprès du SSI; (d) Elle supprime automatiquement tous les comptes désactivés après une période prédéterminée.
	APP-AU.04	Chargement automatique d'un calendrier sur le service vertical web initial destinées au public qui avisera l'utilisateur externe d'événements prédéterminés reliés à des demandes de services aux SSI (p. ex., les dates d'échéance de correspondance et les renouvellements d'inscription des organisations).
Soutien aux opérations	APP-OPS.01	Permet d'appliquer un contrôle des accès avec les autorisations appropriées en fonction des rôles pour tous les utilisateurs et objets définis.
	APP-OPS.02	La solution doit permettre aux utilisateurs internes disposant des autorisations appropriées d'ajouter, de modifier, de désactiver et de supprimer des comptes d'utilisateurs internes et externes.
	APP-OPS.03	Permet aux utilisateurs internes disposant des autorisations appropriées d'ajouter, de modifier, de supprimer ou de désactiver certaines fonctionnalités ou certains rôles des utilisateurs internes et externes.

Catégorie	Section de l'EDT	Exigence
	APP-OPS.04	Permet aux utilisateurs internes disposant des autorisations appropriées d'ajouter, de modifier, de supprimer ou de désactiver les rôles attribués aux utilisateurs dans la solution.
	APP-OPS.05	Permet aux utilisateurs internes disposant des autorisations appropriées d'ajouter, de modifier, de supprimer ou de désactiver les fonctionnalités attribuées aux rôles des utilisateurs.
	APP-OPS.06	Permet aux utilisateurs internes disposant des autorisations appropriées d'ajouter, de modifier, de supprimer ou de désactiver les fonctionnalités qui peuvent être attribuées aux rôles des utilisateurs ou aux utilisateurs.
	APP-OPS.07	Permet aux utilisateurs internes disposant des autorisations appropriées de faire preuve de souplesse et d'adaptabilité afin de mettre en œuvre ultérieurement des politiques, processus et règles administratives et de modifier ceux déjà utilisés par la solution dans son ensemble, c.-à-d. par le service vertical web initial destinées au public externe et par l'application de traitement interne. Par exemple, ces utilisateurs doivent être en mesure de modifier le paramètre de la solution définissant la norme relative au nombre de jours pour remplir une demande d'inscription au PMC. La modification est alors automatiquement reportée dans tous les rapports et tableaux de bord, et utilisée dans tous les calculs internes.
	APP-OPS.08	Permet aux utilisateurs internes disposant des permissions appropriées la flexibilité et l'adaptabilité nécessaires pour ajouter, modifier, supprimer ou désactiver les flux de travaux dans la solution.
	APP-OPS.09	Permet aux utilisateurs internes disposant des autorisations appropriées de gérer les formulaires opérationnels servant au traitement des cas. Par exemple, les utilisateurs privilégiés peuvent ajouter de nouveaux champs de données aux formulaires permettant la saisie de renseignements supplémentaires. De même, ces utilisateurs doivent être en mesure de désactiver les champs de données désormais inutiles.
	APP-OPS.10	Permet aux utilisateurs internes disposant des autorisations appropriées de pouvoir modifier les formulaires externes et les publier sur le service vertical web initial destinées au public.
	APP-OPS.11	Permet aux utilisateurs internes disposant des autorisations appropriées d'ajouter, de modifier, de supprimer ou de désactiver, en tout ou en partie, les modèles utilisés pour la solution (p. ex., les modèles de correspondance).
	APP-OPS.12	Permet aux utilisateurs internes disposant des autorisations appropriées de pouvoir modifier les certificats produits par le système, comme le certificat d'enquête de sécurité, le certificat d'inscription au Programme des marchandises contrôlées, etc.
	APP-OPS.13	Permet le suivi automatisé des dossiers à chaque étape du processus ou du flux de travaux (p. ex., les barres indiquant la progression, le pourcentage ou le temps restant).
	APP-OPS.14	Permet le suivi automatisé des demandes externes et des dossiers de service soumis au SSI à chaque étape (p. ex., les barres indiquant la progression, le pourcentage ou le temps restant).

Catégorie	Section de l'EDT	Exigence
	APP-OPS.15	Permet un triage et un système de déclenchement automatisés des demandes de service en vue d'optimiser le traitement des demandes (seules les exceptions devront faire l'objet d'une intervention manuelle). Par exemple, à la réception d'une demande de service et selon son type, la demande pourrait être triée automatiquement en fonction des données entrées et attribuée à une équipe de traitement désignée (par exemple, une vérification de la fiabilité simple ou une attestation de sécurité du personnel classifiée). Comme autre exemple, lorsqu'une étape du processus est terminée, la demande de service peut être automatiquement attribuée au préposé suivant qui poursuivra son traitement (p. ex., une activité d'inspection peut être déclenchée lorsque l'organisation et le personnel ont reçu l'attestation de sécurité).
	APP-OPS.16	Permet le regroupement automatisé des cas de conformité en fonction de l'emplacement en vue de faciliter l'attribution et le traitement de la charge de travail.
	APP-OPS.17	Permet d'avoir un processus d'établissement de catégories automatisé en fonction des risques ou lorsqu'une mesure de suivi est requise pour faciliter le traitement et éviter les retards superflus.
	APP-OPS.18	Permet d'avoir un processus automatisé d'établissement de la priorité des demandes de service en fonction des priorités opérationnelles prédéterminées ou des exigences de l'industrie évaluées (p. ex., une demande d'autorisation de sécurité urgente pour l'OTAN qui requiert un traitement prioritaire).
	APP-OPS.19	Permet aux utilisateurs internes disposant des autorisations appropriées de pouvoir faire une copie d'une demande de service en lecture seule en cours afin de faciliter le traitement des demandes de renseignements et d'inscription. La demande de service copiée devrait afficher les mêmes éléments que celle que l'utilisateur externe consulte sur le service vertical web initial destinées au public. Cela permet à l'utilisateur interne de voir ce que l'utilisateur externe voit à l'écran et vice versa.
	APP-OPS.20	Permet aux utilisateurs internes disposant des autorisations appropriées de gérer le contrôle de l'accès et les autorisations relatives aux champs selon le rôle de l'utilisateur. Par exemple, un champ peut avoir un accès en écriture pour un rôle d'utilisateur, mais être en lecture seule pour un autre rôle. Dans un autre cas, le champ peut ne pas être visible pour un rôle d'utilisateur donné. Les autorisations relatives aux champs doivent toujours être le plus restrictives possible.
	APP-OPS.21	Permet aux utilisateurs internes disposant des autorisations appropriées de pouvoir, sur demande, mettre à jour un environnement de mise à l'essai avec une copie de la solution de production afin de rafraîchir cet environnement.
	APP-OPS.22	Permet aux utilisateurs internes dotés des autorisations appropriées d'activer ou de désactiver le lien de l'utilisateur externe vers l'environnement de mise à l'essai ou de formation. Voir l'exigence opérationnelle WP-EU 22.

Catégorie	Section de l'EDT	Exigence
	APP-OPS.23	Environnements de la solution : les utilisateurs internes disposant des autorisations appropriées devraient pouvoir accéder aux différents environnements qui seront mis en œuvre pendant le projet de TSSI, les modifier et y permettre l'accès. L'objectif serait de mettre en œuvre les changements opérationnels futurs, de les tester et de les lancer dans un environnement de préproduction pour la préparation du lancement, la migration des changements opérationnels testés et acceptés vers la production, etc. Ces environnements de la solution comprennent notamment : (a) développement; (b) essais; (c) essais d'acceptation par les utilisateurs; (d) préparation; (e) production.
	APP-OPS.24	Permet le versionnage des configurations et la capacité pour le redéploiement des versions de production antérieures de la solution, et non la solution entière dans le cas où un changement mis en oeuvre crée un problème dans une section. Une telle fonctionnalité serait limitée aux utilisateurs internes disposant des autorisations appropriées.
	APP-OPS.25	La solution devra fournir des identificateurs uniques pour les objets système, tels que les cas et les entreprises, qui peuvent être visualisés et mentionnés par les clients internes et externes.
Expérience utilisateur	APP-UE.01	Permet aux utilisateurs internes d'avoir accès à plusieurs flux de travaux et plusieurs dossiers et de les parcourir.
	APP-UE.02	Permet d'offrir à l'utilisateur interne une assistance intégrée à la solution notamment sous la forme de caractéristiques comme des infobulles, des objets interactifs à l'écran, des procédures d'exploitation uniformisées ou des messages du système clairs et concis. Par exemple, si un utilisateur interne place le curseur de sa souris sur un champ du formulaire, une aide contextuelle s'affiche.
	APP-UE.03	Permet à un système de calendrier synchronisé qui avisera les utilisateurs internes d'événements prédéfinis reliés aux demandes de service reçues (p. ex., les dates d'échéance de la correspondance ou le calendrier des inspections).
	APP-UE.04	Prend en charge au moins 1 000 utilisateurs internes simultanément.
	APP-UE.05	La solution doit offrir un soutien pour la navigation dans le contenu.
	APP-UE.06	Les interfaces d'application des utilisateurs internes doivent être disponibles et présentées à l'utilisateur dans la langue officielle de son choix.
	APP-UE.07	Permet de fournir, permettre et soutenir la capacité d'autoriser tous les utilisateurs internes à choisir la langue d'exploitation par défaut dans leur profil. (a) Ce choix inclut les interfaces en anglais et en français. (b) Ce choix doit donner accès à une interface utilisateur en anglais ou en français, au choix de l'utilisateur.
	APP-UE.08	Permet et soutient la capacité de stocker, de traiter et de livrer l'information, les données, les métadonnées et le contenu dans les deux langues officielles du Canada.

Catégorie	Section de l'EDT	Exigence
Gestion de l'information	APP-IM.01	Permettre aux utilisateurs internes accès aux documents justificatifs stockés dans la solution, conformément à leurs besoins opérationnels et aux autorisations qu'ils possèdent (contrôle de l'accès en fonction des rôles);
	APP-IM.02	Permettre aux utilisateurs internes de gérer les documents justificatifs pendant tout le cycle de vie du dossier, conformément aux privilèges qui leur ont été attribués.
	APP-IM.03	Permet aux preuves documentaires d'être protégées contre l'accès, la modification ou la suppression non autorisés.
	APP-IM.04	Permet d'accorder les utilisateurs internes de la solution le minimum de droits d'accès dont ils ont besoin pour exécuter sans entraves leur travail.
	APP-IM.05	Permet d'assurer que les documents ne sont accessibles qu'aux utilisateurs le nécessitant, ayant la bonne cote de sécurité ou de fiabilité et détenant l'autorisation pertinente.
	APP-IM.06	Permettre aux utilisateurs internes de vérifier la pertinence d'un document justificatif pour un dossier donné et de déterminer la mesure à prendre appropriée (p. ex., joindre au dossier ou supprimer).
	APP-IM.07	Permettre aux utilisateurs internes d'associer un document à un ou plusieurs dossiers.
	APP-IM.08	Permettre aux utilisateurs internes de chercher des renseignements (éléments de données) dans différents flux de travaux et différents dossiers simultanément.
	APP-IM.9	Permet aux utilisateurs internes de chercher des documents justificatifs stockés dans la solution.
	APP-IM.10	Permet de stocker toutes les pièces de correspondance (p. ex., les courriels ou les notifications) échangées entre les utilisateurs internes et les utilisateurs externes relativement à un dossier et permet à l'utilisateur interne d'utiliser toutes les pièces de correspondance au dossier pour la prise de décision.
	APP-IM.11	Permettre aux utilisateurs internes d'établir des liens entre les dossiers en fonction d'éléments de données précis ou du contenu. Par exemple, une référence croisée entre un dossier et un autre dossier ou plus d'un dossier en utilisant l'identifiant de l'organisation. Cette fonction complète la rationalisation automatisée des données.
	APP-IM.12	Permettre aux utilisateurs internes de fermer (mettre fin à) un dossier en tout temps au cours du cycle de vie.
	APP-IM.13	Permet l'acquisition de données et de renseignements pendant tout le cycle de vie d'un dossier (p. ex., la demande de sécurité d'une organisation pour obtenir l'Autorisation de détenir des renseignements exige la vérification de la conformité préalablement à l'octroi de l'autorisation de sécurité).
	APP-IM.14	Faciliter l'attribution, la réattribution et la redistribution des dossiers en fonction de la disponibilité des ressources, de la priorité du dossier ou de la complexité du dossier (ce qui vient compléter les flux de travaux automatisés).
	APP-IM.15	Faciliter la collaboration dans tous les secteurs d'activité du SSI en permettant aux utilisateurs internes de créer des notes qui contiennent un texte libre et en associant celles-ci à des utilisateurs, des dossiers, des documents justificatifs, un emplacement ou un événement en tout temps pendant le flux de travaux.
	APP-IM.16	Permettre et soutenir l'archivage des dossiers au sein de la solution.

Catégorie	Section de l'EDT	Exigence
	APP-IM.17	Permet de fournir un dépôt de données unique capable de soutenir tous les aspects des services fournis par le SSI.
	APP-IM.18	Permet d'assurer la qualité des données grâce à l'emploi d'outils de validation tels que la validation générale des adresses.
	APP-IM.19	Permet de faciliter le réglage de la date et de l'heure dans un format commun pour mesurer la performance avec précision.
	APP-IM.20	Permet l'échange d'éléments de données communes entre les programmes du SSI ainsi qu'avec d'autres systèmes d'information.
	APP-IM.21	Permet de tenir un dictionnaire de données définies par l'utilisateur ou un dépôt d'information centralisé contenant la signification des données, leurs relations avec d'autres données, leur origine, leur utilisation et leur format.
	APP-IM.22	Permet de faciliter l'emploi d'identifiants communs dans les différents secteurs d'activité du SSI et doit faciliter l'utilisation d'éléments de données communs dans toutes les demandes de services.
	APP-IM.23	Permet l'affichage et l'impression des versions de formulaires à partir desquels la demande de services d'origine a été envoyée.
	APP-IM.24	Permet la correspondance, la planification et le suivi des rendez-vous selon les exigences touchant le traitement des dossiers de cas.
	APP-IM.25	Facilite la capacité de stockage et de gestion de données structurées et non structurées liées aux dossiers.
	APP-IM.26	Permettre aux utilisateurs internes disposant des autorisations appropriés d'apporter toute modification nécessaire aux données d'un dossier de cas (ajout, suppression, modification, chargement, etc.) tout en préservant l'intégrité de l'information.
	APP-IM.27	Permettre aux utilisateurs internes de récupérer les enregistrements archivés d'un dossier de cas pendant une période donnée, en fonction de l'activité. On doit avoir accès aux dossiers archivés au sein de la solution.
	APP-IM.28	Permet aux preuves documentaires historiques d'être disponibles au sein de la nouvelle solution. Par exemple, tous les documents numérisés qui sont stockés sur la solution d'imagerie documentaire de Matane.
	APP-IM.29	Tous les renseignements en transit entre les systèmes de TI et les renseignements inactifs doivent être chiffrés à l'aide de mécanismes de chiffrement approuvés par le CSTC.
Communication	APP-COM.01	Permet de générer automatiquement des notifications internes et externes selon les mesures prises relativement à la demande (p. ex., une fois que l'inspection d'une organisation a eu lieu, l'agent d'inscription affecté au dossier est avisé qu'il doit finaliser l'inscription de l'organisation).
	APP-COM.02	Permettre de générer automatiquement des notifications par le décideur interne quand une décision est requise De même, quand une décision est prise, les utilisateurs internes et externes concernés doivent en être informés.
	APP-COM.03	Permettre aux utilisateurs externes de recevoir automatiquement des notifications normalisées par courriel résultant d'événements préétablis comme des décisions prises au sujet de la demande de services.

Catégorie	Section de l'EDT	Exigence
	APP-COM.04	Permet de conserver un enregistrement de toute la correspondance (contenu compris) relative à une demande de services.
	APP-COM.05	Permet d'accorder aux utilisateurs internes la capacité de diffuser des messages personnalisés à des groupes ciblés d'utilisateurs externes (p. ex., permettre la communication avec les administrations étrangères désignées en matière de sécurité pour avoir l'assurance que des entreprises étrangères sont habilitées).
	APP-COM.06	Permettre aux utilisateurs internes de produire et d'imprimer la correspondance à envoyer par les services postaux (p. ex., la transmission d'un code d'autorisation lors d'une authentification initiale dans le service vertical web initial destinées au public aux personnes autorisées à la Direction des marchandises contrôlées).
	APP-COM.07	Aide à réacheminer les demandes et à planifier la charge de travail en utilisant des notifications aux utilisateurs internes.
Sans papier	APP-PPL.01	Permet l'acquisition, l'entreposage et la communication de renseignements complémentaires (documents justificatifs et correspondance connexe) au format électronique.
	APP-PPL.02	Permet de joindre les documents numérisés aux dossiers de cas.
	APP-PPL.03	Permettre aux utilisateurs internes de soumettre des demandes de services dans le système par le balayage numérique du code à barres 2D généré par le formulaire (pour compléter les fonctionnalités du service vertical web initial destinées au public relatives aux demandes de services soumises par d'autres voies de communication [le courriel, par exemple]; de plus, cela élimine la nécessité d'entrer manuellement les données recueillies dans les formulaires de demande de services déposés).
	APP-PPL.04	Permettre aux utilisateurs internes d'employer des parties de la solution hors connexion (p. ex., un inspecteur du SSI pourra mettre de côté un dossier de cas [comprenant les documents associés], traiter l'information hors connexion au lieu d'inspection et synchroniser ce dossier de cas au moment de la reconnexion).
	APP-PPL.05	Permettre aux utilisateurs internes de compléter l'information aux dossiers de cas dans divers formats (images, vidéo, audio, etc.) (p. ex., durant une inspection de conformité, l'inspecteur pourra prendre des photos ou enregistrer une vidéo pour les annexer directement au dossier de cas).

Catégorie	Section de l'EDT	Exigence
Interconnectivité	APP-ICN.01	Communiquer avec le logiciel d'apprentissage SABA pour assurer la prestation et le suivi des exigences de formation. La solution doit pouvoir transmettre l'information du compte de l'utilisateur à l'environnement SABA, de sorte que les utilisateurs internes et externes puissent accéder au système SABA aux fins de formation. Une fois la formation requise terminée, le système SABA doit pouvoir mettre à jour la solution avec un dossier de la formation suivie, de sorte que les demandes de services puissent être traitées. Logiciel d'apprentissage SABA sert de plateforme standard au Secteur de la sécurité industrielle pour fournir les cours d'apprentissage prolongé pour le Programme de sécurité des contrats et le Programme des marchandises contrôlées. La plateforme comportera différents types de formation (p. ex., salle de cours virtuelle, présentations PowerPoint) dans divers formats et dans les deux langues officielles. Le système SABA s'occupera aussi de la certification, y compris l'administration automatisée des examens. Les rapports et les analyses des activités d'apprentissage seront également générés par le système SABA. La solution doit avoir la capacité d'absorption des mises à jour de SABA se rapportant à la formation pour le traitement des demandes de services.
	APP-ICN.02	Communique avec la solution d'achats électroniques de TPSGC (dans la mesure où elle sera disponible).
	APP-ICN.03	Communique avec la solution de paiement électronique du receveur général, BARG (dans la mesure où elle sera disponible).
	APP-ICN.04	Accéde aux résultats de vérification de casier judiciaire et d'empreintes digitales de la GRC, afin d'établir une correspondance entre une demande de services soumise, les empreintes digitales correspondantes et les résultats obtenus. L'établissement de la correspondance se fait au moyen d'un numéro de contrôle de document unique fourni au demandeur par la GRC; ce numéro doit être fourni dans le cadre des renseignements soumis avec la demande de services. Ce processus doit être automatiquement enclenché lorsqu'une demande de services est soumise avec succès dans l'application de traitement à partir du service vertical web initial destinées au public. Il doit également être disponible sous forme d'option activée sur demande par des utilisateurs internes.
	APP-ICN.05	Communique avec la GRC au sujet des vérifications des antécédents criminels (VAC). Ce processus doit être disponible sur demande. Autrement dit, la solution doit pouvoir soumettre à la GRC les renseignements lui permettant de procéder à une VAC, accepter la réponse concernant la vérification de la GRC, et intégrer cette réponse en vue de la poursuite du traitement ou du processus décisionnel. Ce processus doit découler de l'intervention manuelle d'un utilisateur interne, au besoin. La soumission de l'information à la GRC et la réception de la réponse doivent se faire de manière uniforme et transparente pour l'utilisateur interne.
	APP-ICN.06	Communique avec la GRC pour lui permettre de transmettre sur demande et lorsque requis des renseignements à jour sur la sécurité.

Catégorie	Section de l'EDT	Exigence
	APP-ICN.07	Communique avec le SCRS pour faire une vérification de la loyauté. Ce processus doit être disponible sur demande. Autrement dit, la solution doit pouvoir soumettre au SCRS les renseignements lui permettant de procéder à une vérification de la loyauté, accepter la réponse du SCRS concernant la vérification de la loyauté, et intégrer cette réponse en vue de la poursuite du traitement ou du processus décisionnel. Ce processus doit se faire automatiquement pour les demandes de services qui exigent une évaluation de la loyauté par le SCRS (par exemple les attestations de sécurité de niveau Secret). Un utilisateur interne doit aussi pouvoir lancer manuellement ce processus, au besoin. La soumission de l'information au SCRS et la réception de la réponse doivent se faire de manière uniforme et transparente pour l'utilisateur interne.
	APP-ICN.08	Communiquer avec les agences de vérification du crédit afin d'effectuer des vérifications concernant la situation financière de particuliers. Autrement dit, la solution doit pouvoir soumettre à un fournisseur de services d'enquête sur la situation financière les renseignements lui permettant de procéder à cette enquête, accepter la réponse connexe, et intégrer cette réponse en vue de la poursuite du traitement ou du processus décisionnel. Ce processus doit se faire automatiquement pour les demandes de services qui exigent une enquête sur la situation financière. Un utilisateur interne doit aussi pouvoir lancer manuellement ce processus, au besoin. La soumission de l'information aux agences d'évaluation du crédit et la réception de la réponse doivent se faire de manière uniforme et transparente pour l'utilisateur interne.
	APP-ICN.09	Interface reliée à un fournisseur de validation d'adresses afin d'effectuer ce type de validation.
	APP-ICN.10	
Établissement de rapports et analyses	APP-RP.01	Permettre aux utilisateurs internes de produire des rapports de suivi, de mesure et de performances (p. ex., comparaison du rendement réel au rendement prévu, au rendement établi pour ce secteur d'activité et aux indicateurs du gouvernement).
	APP-RP.02	Permettre aux utilisateurs internes de produire des rapports procurant à la direction des renseignements nécessaires à la prise de décisions.
	APP-RP.03	Permettre aux utilisateurs internes de produire des rapports standards grâce auxquels ils peuvent surveiller leur charge de travail.
	APP-RP.04	Permettre aux utilisateurs internes de produire des rapports sommaires qui calculent les totaux d'un sujet cible en fonction de critères préétablis. Par exemple, le nombre total d'appels au centre d'appels du SSI pour une période précise; ce nombre étant ensuite décomposé en diverses catégories comme l'état, le type, la catégorie, les demandes de renseignements par direction, etc.
	APP-RP.05	Permettre aux utilisateurs internes de produire des rapports qui ciblent un sujet en particulier et fournissent des calculs fondés sur un ensemble de critères préétablis. Par exemple, pourcentage de demandes d'attestation de sécurité soumises dans le respect des normes pour une période précise.

Catégorie	Section de l'EDT	Exigence
	APP-RP.06	Permettre aux utilisateurs internes de produire des rapports personnalisés et complets en fonction de critères qu'ils ont sélectionnés. Par exemple, liste des organisations inscrites au PMC et des coordonnées de leurs personnes-ressources qui se trouvent en Colombie-Britannique.
	APP-RP.07	Permettre aux utilisateurs internes de produire des rapports qui utilisent des cibles ou des sommaires multiples d'autres rapports afin de fournir des analyses à des fins de formation. Par exemple, nombre de demandes d'inscription soumises auprès de la DMC traitées dans le respect des objectifs pour chacune des cinq dernières années, et indication du pourcentage d'augmentation ou de diminution des activités au cours de la même période de déclaration.
	APP-RP.08	Permettre aux utilisateurs internes de produire des rapports qui donnent de l'information sur un sujet en particulier en fonction de critères sélectionnés et qui présentent l'historique des documents relatifs aux activités jusqu'à leur conclusion. Par exemple, traitement de l'historique d'un dossier d'attestation de sécurité donné.
	APP-RP.09	Permettre aux utilisateurs internes dotés des autorisations appropriées d'ajouter un rapport, de le modifier, de le désactiver, de le supprimer, de le promouvoir ou de le rétrograder au besoin.
	APP-RP.10	Permettre aux utilisateurs de produire tous les rapports associés à la solution proposée sans consulter les autres partenaires.
	APP-RP.11	Permettre aux utilisateurs internes de créer des rapports d'interrogation et de les enregistrer pour une utilisation répétée.
	APP-RP.12	Permettre aux utilisateurs internes de promouvoir un rapport ou de le rétrograder, soit de le faire passer de rapport d'interrogation à rapport standard. Ces rapports peuvent alors être inclus dans l'ensemble de rapports standard de la solution, tant à l'externe (service vertical web initial destinées au public) qu'à l'interne (traitement des demandes).
	APP-RP.13	Permettre aux utilisateurs internes de modifier les critères de sélection associés à un rapport. Par exemple, l'utilisateur doit pouvoir ajouter ou retirer des critères de sélection.
	APP-RP.14	Permettre aux utilisateurs internes de modifier les critères de sélection associés à des rapports normalisés mis à la disposition des utilisateurs externes sur le service vertical web initial destinées au public.
	APP-RP.15	Permettre aux utilisateurs internes de contrôler l'accès aux rapports de la solution en fonction du rôle des utilisateurs et des autorisations accordées. Par exemple, un rapport de la solution spécialement conçu à l'intention de l'Unité d'analyse et de recherches du PMC devrait être mis à la disposition du rôle d'utilisateur correspondant uniquement. Au besoin, l'accès à ce rapport pourrait être partagé avec d'autres rôles d'utilisateurs.

Catégorie	Section de l'EDT	Exigence
Mise en œuvre des processus	APP-PI.01	Permet la mise en œuvre des processus opérationnels du SSI, notamment les suivants : (a) services de filtrage de sécurité du personnel; (b) services d'inscription d'organisations; (c) services des inspections et des enquêtes; (d) services de sécurité des contrats (comprenant les demandes de contrôle des visites et des documents); (e) services des marchandises contrôlées; (f) services de sensibilisation des utilisateurs.
	APP-PI.02	Inclut un document sur les exigences détaillées relatives aux besoins opérationnels comprenant une grille de suivi pour les comparer aux exigences de niveau élevé.

Service vertical Web initial destinées au public L'entrepreneur doit livrer un service vertical web initial destinées au public qui comporte, sans s'y limiter, les fonctionnalités suivantes :

Catégorie	Section de l'EDT	Exigence
Centre de service	WP-SH.01	Offre aux utilisateurs externes un accès sécurisé à l'ouverture d'une session.
	WP-SH.02	Utilise des méthodes approuvées par le gouvernement pour l'identification et l'authentification des utilisateurs (p. ex., SJIA, PasseGC, CléGC, maCLÉ).
	WP-SH.03	Prend en charge au moins 1 000 utilisateurs externes simultanément.
	WP-SH.04	Maintient la qualité du service et du rendement des autres exigences à mesure que la base d'utilisateurs s'accroît. Particulièrement en ce qui concerne les exigences *WP-SH.05, WP-SH.06, WP-SH.10, WP-SH.11, WP-SH.12, WP-UE.04, WP-UE.05, WP-UE.06, WP-UE.07 et WP-UE.08***.** (p.ex., la solution ne doit pas être sujette à des délais accrus, des interruptions inattendues ou à la perte de données enregistrées).
	WP-SH.05	Permet l'échange synchronisé d'information entre le service vertical web initial destinées au public et les applications de traitement de services.
	WP-SH.06	Permet aux utilisateurs externes de soumettre et de gérer les demandes de services, notamment : (a) de remplir les formulaires de demande de services; (b) d'enregistrer et de rouvrir les formulaires incomplets; (c) de soumettre les formulaires remplis.
	WP-SH.07	Permet aux utilisateurs externes de télécharger (soumettre) des documents électroniques étayant leurs demandes de services (p. ex., la copie d'un passeport et des plans d'immeuble).

Catégorie	Section de l'EDT	Exigence
	WP-SH.08	Permet une validation exhaustive des données, assurant que tous les éléments de données requis sont complétés avant la soumission de la demande de services.
	WP-SH.09	Les utilisateurs externes ne doivent pas pouvoir soumettre des demandes de services incomplètes.
	WP-SH.10	Permet aux utilisateurs externes de gérer les changements aux demandes de services (p. ex., l'annulation de la demande de services, la mise à jour des renseignements, etc.).
	WP-SH.11	Permet aux utilisateurs externes de voir l'état d'avancement de leurs demandes de services, notamment : (a) de voir les étapes ou activités réalisées; (b) de voir les étapes ou activités en cours; (c) de voir le délai d'achèvement estimé.
	WP-SH.12	Permet aux utilisateurs externes de chercher et de consulter l'information sur des demandes de services antérieures.
	WP-SH.13	Permet aux utilisateurs externes de mettre à jour leurs profils d'utilisateur.
	WP-SH.14	Permet aux utilisateurs externes de télécharger de données d'une demande de services approuvée (p.ex., des certificats de sécurité du personnel).
	WP-SH.15	Permet aux utilisateurs externes de consulter et de télécharger des formulaires de demande de services, des lignes directrices, des guides, etc.
	WP-SH.16	Permet aux utilisateurs externes de consulter l'état d'avancement des demandes de renseignements et des dossiers de services soumis au SSI. Cette fonction serait distincte de celle concernant les demandes de services soumises.
	WP-SH.17	Permet aux utilisateurs externes de personnaliser leurs interactions avec le SSI selon leurs préférences.
Centre de communication	WP-CH.01	Permet aux utilisateurs externes de recevoir des notifications générales et personnalisées au fur et à mesure du traitement de leur demande de services.
	WP-CH.02	Permet aux utilisateurs externes et au SSI d'échanger des messages.
	WP-CH.03	Permet aux utilisateurs externes de télécharger des documents découlant de leurs demandes de services (p. ex., un certificat de formation ou les modalités de sécurité d'un contrat).
	WP-CH.04	Permet aux utilisateurs d'intégrer au contenu Web sous la forme de fonctionnalités telles que des infobulles, des objets interactifs à l'écran, des liens vers les guides, des FAQ et des messages du système clairs et concis.
	WP-CH.05	Offre l'intégration d'un système de calendrier synchronisé qui avisera l'utilisateur externe d'événements prédéterminés reliés à des demandes de services au SSI (p. ex., les dates d'échéance de la correspondance et des renouvellements d'inscription des organisations).
	WP-CH.06	Permet aux utilisateurs externes de type « agent de sécurité » de transmettre les notifications reçues du SSI directement aux utilisateurs finaux de type « demandeur ».

Catégorie	Section de l'EDT	Exigence
	WP-CH.07	Permet aux utilisateurs externes de type « demandeur » d'envoyer des notifications uniquement aux utilisateurs finaux de type « agent de sécurité » qui ont demandé la création de leur compte.
	WP-CH.08	Offre aux utilisateurs externes la possibilité de présenter les demandes de renseignements relatives aux services ou les dossiers de service au SSI. (p. ex., assurer le suivi des demandes de renseignements visant à déterminer pourquoi une attestation de sécurité n'a pas progressé après un certain temps).
Expérience utilisateur	WP-UE.01	Permet aux utilisateurs externes autorisés de demander la création de comptes pour d'autres utilisateurs externes (p. ex., un agent de sécurité doit pouvoir demander la création d'un compte pour une autre personne [demandeur] afin de pouvoir remplir la demande).
	WP-UE.02	Permet aux utilisateurs externes autorisés de remplir une demande de services, de la signer de manière électronique, puis de la soumettre à d'autres utilisateurs externes aux fins d'examen et d'approbation, avant de la présenter au SSI (p. ex., un demandeur doit pouvoir remplir une demande de services, puis la marquer comme signée, ce qui fera en sorte que l'agent de sécurité recevra une demande d'examen et de soumission au SSI aux fins de traitement).
	WP-UE.03	Permet aux utilisateurs externes autorisés (p. ex., un agent de sécurité) de remplir une demande de services au nom d'autres utilisateurs (p. ex., un demandeur). Par exemple, un agent de sécurité remplit une demande d'attestation de sécurité du personnel au nom d'un demandeur. Le demandeur doit signer le formulaire avant que l'agent de sécurité d'entreprise (ASE) puisse signer le formulaire aux fins de soumission.
	WP-UE.04	Permet aux utilisateurs externes autorisés (p. ex., un agent de sécurité) de transmettre une demande remplie au nom d'un autre utilisateur externe (p. ex., un demandeur) aux fins d'examen et de la signature électronique.
	WP-UE.05	Permet aux utilisateurs externes d'employer des appareils mobiles dotés de fureteurs Internet pour accéder au service vertical web initial destinées au public en tout temps. Comprend la signature électronique.
	WP-UE.06	Permet aux utilisateurs externes d'accéder au service vertical web initial destinées au public à partir de tablettes dotées de fureteurs Internet sans perdre aucune des fonctionnalités du service vertical web initial destinées au public.
	WP-UE.07	Permet aux utilisateurs externes d'accéder à une version légère du service vertical web initial destinées au public à partir d'un téléphone intelligent.
	WP-UE.08	Permet aux utilisateurs externes de recevoir des notifications générales, par exemple à propos d'une interruption de service.
	WP-UE.09	Permet aux utilisateurs externes de recevoir des messages courriel normalisés au sujet de mises à jour sur les demandes de services.
	WP-UE.10	Permet accès aux formulaires de demande de services dans un autre format que les utilisateurs externes peuvent télécharger et remplir en dehors du service vertical web initial destinées au public et soumettre au SSI aux fins de traitement.
	WP-UE.11	Donne aux usagers l'accès à des formulaires à remplir téléchargeables qui sont à compléter. Ces formulaires doivent contenir les mêmes champs de données que leurs équivalents en ligne.

Catégorie	Section de l'EDT	Exigence
	WP-UE.12	Permet de transférer les données des formulaires de demande de services dans d'autres formats dans la solution à l'aide d'un code à barres sans saisie manuelle (p. ex., à l'aide de la numérisation d'un code à barres) en corrélation avec les exigences *APP-PPL.01, APP-PPL.02* et *APP-PPL.03.*
	WP-UE.13	Assure un degré élevé d'exactitude au moyen de l'utilisation d'outils de validation des données (p. ex., la validation des adresses globale) et de la fédération des données avec divers partenaires gouvernementaux.
	WP-UE.14	Empêche les utilisateurs externes de soumettre une demande de services en double dans le cas d'une demande déjà en traitement ou complétée. Ainsi, les utilisateurs externes ne doivent pas pouvoir soumettre une demande d'attestation de sécurité de niveau Secret si une telle attestation valide existe déjà.
	WP-UE.15	Assure la flexibilité et l'adaptabilité de la mise en œuvre ultérieure de politiques, processus et règles administratives.
	WP-UE.16	Permet aux utilisateurs externes de signer de manière électronique leurs demandes de services.
	WP-UE.17	Permet aux utilisateurs externes de naviguer dans le service vertical web initial destinées au public d'une manière conforme aux normes pour le Web du GC.
	WP-UE.18	Permet aux utilisateurs externes de pouvoir établir la priorité de leur demande de service en fournissant une justification appropriée qui sera évaluée au cours des activités de traitement.
	WP-UE.19	Permet aux utilisateurs externes de créer des demandes additionnelles à partir de renseignements saisis, lorsque seuls les renseignements pertinents à cette nouvelle demande sont requis. À titre d'exemple, si une personne a déjà soumis une demande d'autorisation de sécurité du personnel et qu'elle souhaite par la suite demander une attestation de sécurité de niveau Secret, elle n'a qu'à fournir les renseignements pertinents à la demande d'attestation de sécurité de niveau Secret, sans entrer de nouveau les renseignements fournis dans le cadre de la demande d'attestation de sécurité du personnel.
	WP-UE.20	Permet aux utilisateurs externes d'enregistrer les formulaires soumis en format PDF, de sorte qu'ils ressemblent au formulaire de demande de services réel.
	WP-UE.21	Permet la validation du formulaire au fur et à mesure que chaque section est remplie, au moyen d'un message clair et concis avisant l'utilisateur externe en cas d'erreur.
	WP-UE.22	Environnement de formation de l'utilisateur externe : Permet aux utilisateurs externes de pouvoir accéder à un environnement public de formation distinct ou à un environnement de mise à l'essai leur permettant de découvrir les services fournis par le SSI et d'apprendre à les utiliser. Cet environnement de formation n'affichera que les fonctionnalités du service vertical web initial destinées au public et ne conservera ni ne transmettra de données.
	WP-UE.23	Fournir, permettre et soutenir la capacité de stocker, gérer et présenter l'information, les données, les métadonnées et contenu dans les deux langues officielles canadiennes.

Catégorie	Section de l'EDT	Exigence
	WP-UE.24	Fournir, permettre et soutenir la capacité de tous les utilisateurs externes de choisir la langue d'exploitation par défaut dans leur profil. (a) Ce choix inclut les interfaces en anglais et en français. (b) Ce choix doit donner accès à une interface utilisateur en anglais ou en français, au choix de l'utilisateur.
	WP-UE.25	Langue de préférence : les interfaces d'application des utilisateurs externes doivent être disponibles et présentées à l'utilisateur dans la langue officielle de son choix.
Établissement de rapports et analyses	WP-RP.01	Rapports d'utilisation : Permet la capacité de recueillir de l'information sur l'utilisation et de produire des rapports connexes, selon les normes du GC.
	WP-RP.02	Permettre aux utilisateurs externes de produire des rapports normalisés en fonction d'un ensemble limité de critères prédéfinis. À titre d'exemple, un rapport qui permet à l'agent de sécurité de visualiser l'état de toutes les demandes d'autorisation de sécurité du personnel de son organisation à l'aide d'un critère de filtre qui permet de choisir une période précise ou toutes les demandes, ou encore un demandeur en particulier.
	WP-RP.03	Permet accès aux rapports disponibles dans les formats PDF, Excel (XLS, XLSX) et Word (DOC, DOCX) aux fins de téléchargement et d'impression par l'utilisateur externe.
	WP-RP.04	Permet aux utilisateurs externes d'enregistrer ou imprimer les rapports sur demande.

2.2.3 Migration des données

L'entrepreneur doit fournir et livrer les activités suivantes pour la migration des données :

Catégorie	Section de l'EDT	Exigence
Migration des données	APP-MD.01	Élaborer une stratégie de migration de données qui inclut des considérations clés et fournit des recommandations par rapport à l'approche des activités de migration de données. Notez que l'entrepreneur n'effectuera pas la migration finale des données, ce sera effectué par TPSGC DDPI / SPC.

Catégorie	Section de l'EDT	Exigence
	APP-MD.02	Élaborer un plan de migration de données qui inclut: (a) Une description détaillée de toutes les activités requises pour compléter la migration des données des systèmes existants vers la solution, y compris: i. L'analyse des données ; ii. Développement / configuration des outils de migration; iii. Evaluation de la migration; iv. Validation de la migration des données; v. Documentation de la migration des données. (b) Un calendrier pour l'achèvement de toutes les activités de migration de données élaborées. Le calendrier proposé doit respecter les délais indiqués dans le calendrier du projet. (c) Une estimation du nombre et des catégories de ressources nécessaires pour mener chaque activité de migration et une répartition des coûts associés.
	APP-MD.03	Documenter une cartographie de toutes les données nécessitant une migration vers la nouvelle conception architecturale. La cartographie doit être mise à jour dans l'éventualité où l'architecture du système soit modifiée.
	APP-MD.04	Aider le gouvernement du Canada en matière d'orientation et de documentation pour la migration de l'échantillon de données et la validation des données. Évaluer l'intégrité des données et l'incidence de la migration. L'échantillon de données doit inclure 50 dossiers de chaque processus, p. ex. le personnel de contrôle de sûreté, marchandises contrôlées, etc. Ces conclusions doivent être signalées au responsable du projet, indiquant le niveau de réussite de l'approche pour la migration des données.
	APP-MD.05	Documenter toutes les étapes requises pour la mise en œuvre du plan de migration de données. Maintenir les documents à jour dans le cas où l'architecture du système est modifiée.

PARTIE 3 : EXIGENCES TECHNIQUES

Cette section définit les exigences techniques pour la solution.

1.1 APERÇU DES EXIGENCES

L'entrepreneur doit concevoir, élaborer, configurer, mettre à l'essai, mettre en œuvre, déployer et stabiliser une solution fondée sur des exigences précises, l'architecture conceptuelle de la solution ISST de haut niveau et l'utilisation des technologies énumérées dans cet énoncé des travaux. La solution doit être conviviale, fiable, adaptable, extensible, interopérable et extensible de manière à pouvoir être ajustée en fonction des processus opérationnels ayant fait l'objet de modifications, d'adaptations ou d'ajouts ainsi que des fonctions automatisées du système. La solution doit également être conforme aux politiques, aux lignes directrices et à l'environnement du GC en matière de TI-GI.

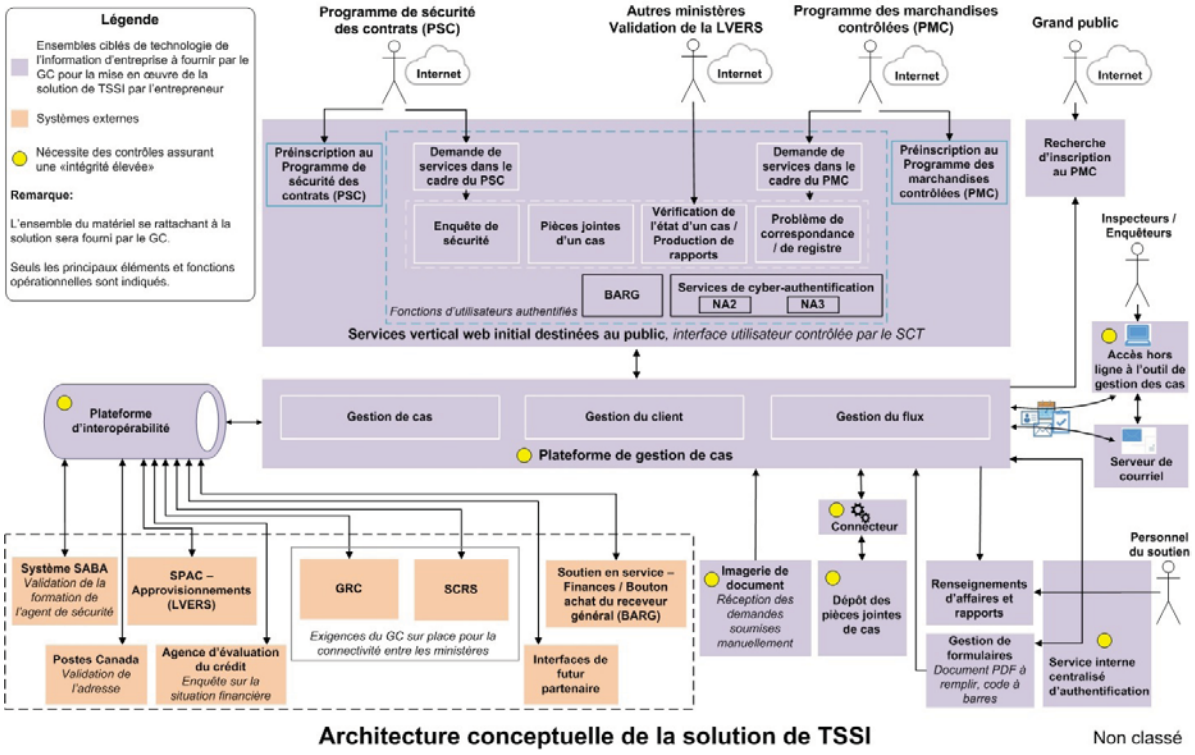


Figure 2: Diagramme d'architecture de la solution ISST de haut niveau.

Microsoft Dynamics CRM est la principale plateforme de la solution du SSI offrant des capacités comme la gestion des cas et des clients, de même que des flux de travaux à des fins d'automatisation des processus opérationnels. L'accès à cette plateforme devra être accordé au personnel de soutien du SSI une fois qu'il aura été authentifié au moyen du service d'authentification d'accès sécurisé. Les inspecteurs sur le terrain pourront aussi interagir avec la plateforme principale MS Dynamics CRM à l'aide de capacités d'accès hors ligne reposant sur Microsoft Dynamics CRM pour Outlook.

Les utilisateurs externes, par exemple les demandeurs du Programme de la sécurité des contrats et du Programme des marchandises contrôlées, auront accès à la fonctionnalité requise pour leurs processus opérationnels par l'intermédiaire des services Web de première ligne, verticaux et accessibles au public. Ces utilisateurs auront accès à l'environnement après avoir été authentifiés selon le niveau d'assurance approprié requis par l'application à l'aide des services d'authentification électronique et en fonction de rôles et de droits bien précis. **Aucun** accès direct à la plateforme principale MS Dynamics CRM ne sera accordé aux utilisateurs externes. La plateforme des services Web de première ligne, verticaux et accessibles au public permettra d'héberger des formulaires Web conçus pour la demande et la réception des services. La configuration des services Web de première ligne, verticaux, accessibles au public et habilitant les interfaces des processus opérationnels liés à la réception des demandes doit satisfaire aux exigences du GC (WCAG) en matière de normes Web.

L'entrepreneur devra configurer la technologie qui résidera sur le réseau du GC, ainsi que l'interface avec la plateforme de gestion des cas Dynamics CRM. La solution devra être extensible de manière à répondre aux besoins du développement futur, reposer sur les services Web et privilégier principalement la configuration par rapport à la personnalisation.

L'accès des utilisateurs aux différentes fonctionnalités de l'application sera accordé au moyen des privilèges et des configurations d'accès fondés sur le rôle des plateformes technologiques sous-jacentes en fonction des profils d'accès des utilisateurs.

La solution doit tirer parti de la technologie décrite par TPSGC dans la liste descriptive ci-dessous. Ces technologies sont des suites cibles de TI d'entreprise qui sont dictées par les directions du dirigeant principal de l'information (DDPI) du SCT ou de TPSGC, afin de réduire et de rationaliser l'empreinte des applications du GC et de TPSGC. Dans la mesure du possible, l'entrepreneur doit satisfaire aux exigences de la solution, ainsi qu'à toutes les nouvelles exigences découlant de la restructuration des processus opérationnels en mettant à profit ces technologies de manière à développer une solution unifiée.

Les suites cibles de TI d'entreprise mentionnées auxquelles l'entrepreneur doit se conformer comprennent, entre autres, les suivantes :

(a) Dynamics CRM (sur place) 2015 (ou version ultérieure) (suite cible de TI d'entreprise) Technologie de gestion des cas – Les services Web de première ligne, verticaux et accessibles au public pour la réception des demandes des entreprises permettront d'échanger des informations avec un outil de gestion des relations avec la clientèle, MS Dynamics CRM (sur place) 2015 (ou version ultérieure), afin d'entreprendre, de gérer et d'exécuter des activités de gestion de cas et d'échanger des informations à ce sujet. L'outil de gestion des cas est un service géré de façon centralisée et sera utilisé par les utilisateurs internes ayant des rôles et des droits bien définis.

(b) Microsoft Exchange Server, Client d'Outlook (suite cible de TI d'entreprise) et MS Dynamics CRM pour le courriel Outlook du GC – Cette technologie servira à soutenir les capacités de courriel et de gestion des cas hors ligne pour les utilisateurs internes, comme les inspecteurs sur le terrain.

(c) Business Objects de SAP (suite cible de TI d'entreprise) Établissement de rapports relatifs aux renseignements d'affaires – La suite Business Objects BI de SAP permet aux entreprises de réaliser des analyses opérationnelles. En ce qui concerne cette solution, toutefois, les fonctionnalités comprenant des tableaux de bord destinés aux utilisateurs internes mettront d'abord à profit les

capacités d'établissement de rapports qu'offrent les outils de Dynamics CRM 2015 (ou une version ultérieure). Si ces derniers ne permettent pas d'établir des rapports stratégiques, la suite Business Objects BI de SAP, reliée à un entrepôt de données pures, effectuera cette tâche. Les fonctions de production de rapports doivent être mises à la disposition des utilisateurs internes et externes selon les profils d'accès des utilisateurs.

(d) Service Bus d'Oracle (suite cible de TI d'entreprise) Technologie de partage de l'information – Plateforme d'interopérabilité du GC (PIGC – basée sur Service Bus d'Oracle (technologie). Le partage de l'information entre le Secteur de la sécurité industrielle (SSI) et les organisations partenaires doit être automatisé et géré selon les capacités de la PIGC et de la technologie sous-jacente de Service Bus d'Oracle.

(e) Système d'imagerie et de numérisation – Ce système est en place et utilise la technologie DataCap d'IBM. La solution de l'ISST devra permettre l'échange de l'information avec ce système.

(f) Système de gestion des documents et des dossiers – La solution devrait nécessiter l'entreposage, la gestion et l'extraction des données regroupées principalement en deux catégories : (1) Système de gestion des bases de données ou des données – Données structurées faisant l'objet d'un grand nombre d'opérations de traitement et de transactions, habituellement associées aux demandes en cours de traitement et aux données sur les entreprises et le personnel; et (2) Système de gestion des documents et des dossiers – Données non structurées habituellement associées à des pièces jointes qui ne doivent pas être modifiées, mais qui doivent être conservées à des fins de gestion des documents et des dossiers et à des fins de preuve (p. ex., passeports, certificats de naissance, etc.), ce qui représente un volume inférieur de transactions ainsi qu'un faible taux d'extraction de données.

i) **Système de gestion des bases de données ou des données** – L'entrepreneur doit tirer parti des produits existants déjà autorisés et utilisés par SPAC, afin de satisfaire aux exigences liées au traitement de l'information et des données non sensibles, sensibles et intensives. La solution doit respecter les normes de SQL Server ou d'Oracle du GC pour toutes les applications de bases de données.

ii) **Système de gestion des documents et des dossiers** – La norme actuelle du GC pour la gestion des documents et des dossiers est Content Server d'OpenText, qui devrait être utilisée pour l'entreposage à long terme des données non structurées. Il s'agit de la valeur par défaut pour les éléments qui ne sont pas nécessaires au traitement dynamique, tels que (sans toutefois s'y limiter) les pièces jointes statiques et les formulaires soumis en personne qui sont numérisés à des fins de gestion des documents et des dossiers.

L'entrepreneur doit assurer une expertise technique en matière de GI-TI dans les domaines relatifs au développement des applications, notamment en ce qui touche le langage de programmation C# et Java, la configuration et l'intégration, la restructuration des processus opérationnels, l'intégration de l'information, ainsi que la sécurité des applications et des données.

L'ensemble du matériel se rattachant à la solution sera fourni par le GC et aucune autre installation matérielle (outre celles que requiert la connectivité au réseau) ne sera nécessaire. Si l'entrepreneur utilise des outils logiciels ne se trouvant pas dans le GC, il lui faut faire approuver ces outils par le GC avant de commencer le processus

d'installation pour TPSGC. L'entrepreneur doit travailler en étroite collaboration avec Services partagés Canada (SPC) pour faire en sorte que les capacités matérielles respectent ou surpassent les exigences de la solution globale.

1.2 EXIGENCES TECHNIQUES

L'entrepreneur doit mettre en œuvre une solution qui réponde, sans pour autant s'y limiter, aux exigences énumérées ci-dessous.

Section de l'EDT	Exigence
Tech.01	Mettre en œuvre les pages Web dont le codage est UTF-8.
Tech.02	Mettre en œuvre l'intégration en temps réel au moyen d'une architecture de services Web telle que REST (HTTP, codage JSON ou XML) et SOAP (HTTP ou JMS).
Tech.03	Permettre aux utilisateurs externes d'exporter les résultats, notamment des rapports et des résultats de recherche, sous forme de tableau ou de graphique, dans tous les formats qui satisfont spécifiquement aux exigences des WCAG 2.0 et assurer la mise en œuvre du processus d'exportation.
Tech.04	Respecter les pratiques exemplaires de sécurisation des services Web, comme celles du guide sur les services Web sécurisés (publication spéciale 800-95 du National Institute of Standards and Technology [NIST]) et de la deuxième version des directives sur la sécurisation des serveurs Web publics (publication spéciale 800-44 du NIST).
Tech.05	Permettre la fermeture automatique d'une session Web ouverte après un délai d'inactivité qui sera fixé par le GC et assurer la mise en œuvre du processus de fermeture.
Tech.06	Permettre aux utilisateurs internes d'exporter les résultats, notamment des rapports et des résultats de recherche, sous forme de tableau ou de graphique, dans les formats de fichier suivants qui satisfont aux techniques énoncées dans les WCAG 2.0 (https://www.canada.ca/fr/secretariat-conseil-tresor/services/communications-gouvernementales/boite-outils-experience-web.html) en ce qui a trait aux essais de conformité : (a) PDF (PDF d'Adobe); (b) DOC, DOCX (MS Word 2013 et version ultérieure); (c) XLS, XLSX (MS Excel 2013 et version ultérieure).
Tech.07	Mettre en œuvre la solution afin de prendre en charge la norme la plus récente du GC en matière de navigateur Web (à l'heure actuelle, Microsoft Internet Explorer 11), ainsi que deux versions précédentes d'importance du navigateur Microsoft à mesure qu'évoluent les normes.
Tech.08	Mettre en œuvre une solution compatible avec les principaux navigateurs Web qui prennent en charge le protocole de chiffrement TLS 1.2 offert sur le marché à l'heure actuelle (tels Firefox, Safari et Chrome, pour ne nommer que ceux-là). Consulter le glossaire (Appendice 5 de l'Annexe A) afin d'obtenir plus de renseignements.

Section de l'EDT	Exigence
Tech.09	Proposer une solution sécurisée axée sur un navigateur Web dont l'installation sur le poste de travail de l'utilisateur interne ne requiert aucun autre logiciel de bureau que le navigateur Web, « Microsoft Dynamics CRM for Outlook » afin d'assurer la gestion des cas hors ligne, et MS Outlook.
Tech.10	Mettre en œuvre l'acceptation et le téléchargement de documents d'appui et de pièces jointes dont la taille maximale pourrait excéder 30 mégaoctets, ainsi que de tous les formats de fichiers.
Tech.11	Mettre en œuvre la validation et la confirmation de la saisie des données selon le type de champ, la taille des données, les propriétés du tableau et la liste des valeurs préconfigurées (p. ex., pour le code postal, seul le format valide sera accepté).
Tech.12	Utiliser les services Web de première ligne, verticaux et accessibles au public pour faciliter les processus de réception des demandes des entreprises, comme la création de formulaires Web pour recueillir et échanger de l'information, et qui sont intégrés aux entités MS Dynamics CRM 2015 (ou version ultérieure) et qui prennent en charge les techniques Tech14 et Tech.18.
Tech.13	Offrir un style d'architecture permettant une bonne gestion des erreurs, la restauration et la notification aux utilisateurs lorsque des erreurs se produisent en ligne.
Tech.14	Par souci de convivialité, intégrer les pratiques exemplaires quant aux principes de conception des applications Web (en d'autres termes, mettre à profit les meilleures pratiques en matière d'applications Web [W3] : boutons d'activation et de désactivation, options et transmission des données fondées sur les valeurs saisies par l'utilisateur, réduction des messages-guides inutiles, etc.).
Tech.15	Utiliser au maximum la fonction intégrée d'établissement de rapports de l'application MS Dynamics CRM 2015 (ou d'une version ultérieure) pour permettre à la communauté des utilisateurs internes d'établir des rapports opérationnels et de se servir du tableau de bord et, dans la mesure du possible, de préparer des rapports stratégiques.
Tech.16	Tirer parti de la capacité de la plateforme de renseignements d'affaires du GC pour mettre en œuvre des fonctions d'établissement de rapports que n'offre pas la solution axée sur MS Dynamics CRM (sur place) 2015 (ou une version ultérieure). L'entrepreneur devra pour ce faire créer des scripts d'extraction, de transformation et de chargement (ETC) qui copieront automatiquement les données de la base de données de la solution pour les intégrer à la plateforme de renseignements d'affaires du GC et doter ainsi cette dernière de fonctions relatives à l'établissement de rapports et au tableau de bord. L'entrepreneur développera ces fonctions de telle sorte qu'elles puissent soutenir les décisions opérationnelles.
Tech.17	Satisfaire aux exigences pertinentes du profil de sécurité « Protégé B, Intégrité élevée, disponibilité moyenne » (PB/É/M) pour les plateformes indiquées dans le diagramme de l'architecture conceptuelle de l'ISST.

Section de l'EDT	Exigence
Tech.18	Assurer la conformité aux normes Web du GC (https://recherche-search.gc.ca/rGs/s_r?cdn=canada&st=s&num=10&langs=en&st1rt=1&s5bm3ts21rch=x&q=web+standards&_charset_=utf-8&wb-srch-sub=) et aux normes sur l'accessibilité des sites Web (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601) pour les processus de réception des demandes des entreprises reposant sur les services Web de première ligne, verticaux et accessibles au public.
Tech.19	Favoriser l'extensibilité, si une extension de la communauté d'utilisateurs ou une fonctionnalité de la solution est nécessaire pour soutenir les initiatives du GC.
Tech.20	Fournir une réponse sous la forme d'un accusé de réception ou d'un numéro de cas à un utilisateur externe dans un délai acceptable (en temps quasi réel) après la réception d'une demande unique correctement remplie (le GC déterminera le délai de réponse acceptable).
Tech.21	Créer et transmettre des renseignements aux utilisateurs au moyen d'avis.
Tech.22	Appuyer le concept d'architecture ouverte et donner l'accès à ses services et à ses fonctions au moyen d'API, de services Web et de technologies similaires.
Tech.23	Au cours de la période de transition, favoriser l'échange de données à partir des systèmes en place et vers ceux-ci par les moyens suivants : (a) temps quasi réel ou lots; (b) services Web ou API; (c) langage XML ou fichier non hiérarchique; (d) exportation et importation des données et du contenu; (e) messagerie d'entreprise ou ESB.
Tech.24	Recourir aux Services gérés de transfert sécurisé de fichiers (SGTSF) pour faire passer les fichiers numérisés dans le Système partagé de gestion des cas (SPGC).
Tech.25	Favoriser l'intégration par l'insertion de formulaires PDF intelligents ou à codes à barres auxquels l'utilisateur accède manuellement, ou à l'aide d'autres outils de numérisation afin de faciliter le traitement des cas sur support papier.
Tech.26	Tirer parti et soutenir des normes et des pratiques exemplaires de l'industrie des technologies de l'information et du GC qui ont été adoptées à grande échelle pour la création et le maintien d'un système informatique performant afin de répondre aux besoins suivants : (a) Fournir des applications Web conviviales; (b) Assurer et maximiser la maintenabilité de la solution; (c) Assurer et atteindre un niveau de fiabilité élevé; (d) Assurer l'extensibilité et la viabilité; (e) Garantir un niveau de performance acceptable du système

Section de l'EDT	Exigence
Tech.27	Soutenir les plans stratégiques du GC au chapitre de l'interopérabilité des applications, y compris, à tout le moins, par les moyens suivants : (a) en présentant ses fonctionnalités par l'intermédiaire d'une API qui tire parti des protocoles d'API conformes aux normes de l'industrie (ces fonctionnalités comprennent la capacité d'afficher au besoin les processus opérationnels contenus dans la solution); (b) en respectant les normes du GC – la Plateforme d'interopérabilité du GC (PIGC) qui sera normalisée selon la technologie de service Oracle Bus.
Tech.28	Interagir avec les éléments de technologie de l'information du GC (p. ex., l'infrastructure et la plateforme) sans qu'il soit nécessaire de transformer l'infrastructure existante du GC ou de modifier les postes de travail. Voici une liste des types de technologies qui devraient être pris en charge : (a) SAML 2.0 (b) JSON (c) Kerberos (d) X.509 (e) LDAP (f) CAFR (contrôle d'accès fondé sur les rôles) (g) OAuth (h) SOAP (i) REST (j) OData
Tech.29	Prendre en charge, utiliser ou développer des interfaces externes structurées et modulaires qui permettront l'échange de renseignements entre la solution et les autres systèmes par l'intermédiaire d'une infrastructure de communication sécurisée. Ces interfaces comprennent à tout le moins : a) Un intranet ou un extranet pour les processus opérationnels décrits dans la partie 2, « Exigences opérationnelles »; b) Des services Web – source de données de tiers; c) Des composantes de sécurité de tiers offertes sur le marché, par exemple des produits d'infrastructure à clés publiques (ICP); d) Des systèmes du GC ou des organisations non gouvernementales contenant les renseignements à l'appui nécessaires au traitement des transactions.
Tech.30	Interagir avec d'autres systèmes et plateformes comme l'indique au figure 2, en utilisant à tout le moins les éléments suivants : (a) API; (b) exportation et importation des données et du contenu; (c) messages utilisant le protocole Simple Object Access (SOAP) ou échanges de fichiers au moyen de l'Enterprise Service Bus [ESB] d'Oracle.

Section de l'EDT	Exigence
Tech.31	Inclure la protection des données transactionnelles en transit et statiques par le recours au Centre de la sécurité des télécommunications Canada (CSTC), à des algorithmes de chiffrement approuvés par le SCT ou par d'autres moyens que le GC estime acceptables.

L'entrepreneur doit :

Section de l'EDT	Exigence
Tech.32	Établir et soutenir, pour la durée du contrat et suivant les besoins, des environnements de simulation distincts au niveau de l'application aux fins de configuration, de mise à l'essai, de déploiement ainsi que de formation relativement aux nouvelles versions de la solution. Après le lancement de la solution, ces environnements demeureront en tout ou en partie et seront utilisés pour les activités en cours : l'entrepreneur devra donc assurer le transfert sans heurt des environnements configurés au GC.
Tech.33	Concevoir, développer, configurer, mettre à l'essai et prendre en charge la base de données de la solution afin de stocker, de gérer et de protéger les données allant jusqu'au niveau Protégé B.
Tech. 34	Élaborer des plans d'architecture logique et physique de l'ISST (à l'aide de modèles GC) en fonction du modèle d'architecture conceptuelle ISST. Ces plans sont soumis à l'approbation du GC.
Tech.35	Transférer au personnel de TPSGC les connaissances techniques liées au système et veiller à remettre au Ministère des copies de toute la documentation qui s'y rattache, y compris, mais sans s'y limiter, les documents portant sur la sécurité, la configuration fonctionnelle et non fonctionnelle, les livrets de conception et les dossiers d'exploitation et cela, avant l'achèvement des travaux.
Tech.36	Concevoir et créer une architecture de données présentant les caractéristiques suivantes : (a) inclut tous les modèles de données conceptuels, logiques et physiques pertinents; (b) définit, en collaboration avec TPSGC, les politiques, les règles et les normes liées à la gouvernance des données, notamment la façon dont celles-ci seront stockées, organisées, intégrées et mises à profit dans le cadre de la solution; (c) inclut des dictionnaires de données; (d) fonctionne dans l'environnement de la solution du SSI; (e) soutient l'ensemble des processus opérationnels du SSI; (f) soutient les exigences en matière de sécurité décrites dans le présent document (consulter la partie 5, qui porte sur les exigences relatives à la sécurité de la TI).
Tech.37	En collaboration avec le GC, effectuer la mise en correspondance des données des systèmes en place et de celles de la solution, et procéder à l'analyse des écarts.

Section de l'EDT	Exigence
Tech.38	Développer la documentation d'interface détaillée, incluant, mais sans s'y limiter: (a) Concept des opérations; (b) Vue d'ensemble des systèmes; (c) Vue d'ensemble de l'interface (pour chaque Interface dans, vers et de l'application); (d) Allocation fonctionnelle; (e) Transfert de données; (f) Transactions; (g) Sécurité et intégrité; (h) Exigences relatives à l'interface; (i) Exigences relatives au temps de traitement de l'interface; (j) Exigences relatives aux messages (ou fichiers); (k) Méthodes de communication; (l) Exigences de sécurité; (m) Méthodes de qualification; (n) Approbations; (o) Registre des changements.
Tech.39	Permettre la gestion des formulaires au moyen de la configuration dans *Dynamics* (ou un autre moyen) sans avoir besoin d'un développeur.
Tech.40	Acheter et configurer une technologie commerciale de portail Web qui satisfait aux exigences de la demande de soumissions actuelle.
Tech.41	Installer et exécuter sur *Windows Server 2012* et le serveur Web Internet Information Services (IIS).
Tech.42	Exploiter majoritairement; configuration par rapport à personnalisation.
Tech.43	Se rattacher au réseau du GC et être échelonnable.
Tech.44	Être configurable pour permettre l'intégration des justificatifs de la Fédération des justificatifs du gouvernement du Canada (FJGC).
Tech.45	Interface/intégration uniforme avec *MS Dynamics CRM* (2015 ou version plus récente) au moyen de services Web et/ou d'autres méthodes approuvées et soutenues par les plateformes de technologie sous-jacentes pour son intégration à la plateforme de gestion des cas *Dynamics CRM*.
Tech.46	Permettre la création et la publication de contenu dans les deux langues officielles du Canada, soit le français et l'anglais.
Tech.47	Configurer une solution qui répond aux exigences de la demande de soumissions en cours.
Tech.47A	Fournir des spécifications de conception détaillées.
Tech.47B	Fournir une approche relative à la gestion des relations, incluant les éléments suivants : a) Approche globale relative à la gestion des relations entre le gouvernement et l'entrepreneur; b) Communications entre le gouvernement du Canada et l'entrepreneur en ce qui a trait au un modèle de gouvernance et à la structure de l'équipe proposés, comme défini au point A du C1; c) Gestion et résolution de problèmes; d) Planification mixte et gestion des changements à la portée et au calendrier du projet

L'entrepreneur doit utiliser un service de front-end pour la technologie d'admission d'entreprise qui:

Tech.48	Permettre le chiffrement.
Tech.49	L'entrepreneur doit concevoir la solution pour veiller à ce que des « signatures numériques » soient utilisées à la fois pour les processus entamés par un utilisateur interne et par un service interne, au besoin.
Tech.50	L'entrepreneur doit déterminer et décrire, en tenant compte de la conception de son architecture physique, les contrôles de sécurité qui doivent être mis en œuvre par l'entrepreneur et le GC.
Tech.51	L'entrepreneur doit définir le contenu de la solution et configurer celle-ci afin de produire des dossiers de vérification générés par le système qui comprendront de l'information pour faciliter la détermination des infractions à l'intégrité.
Tech.52	Assurer l'échange de l'information et une intégration avec MS Dynamics CRM (2015 ou version ultérieure) à l'aide des services Web ou d'autres méthodes approuvées et prises en charge par les plateformes technologiques sous-jacentes pour assurer l'intégration de la solution avec la plateforme de gestion des cas de Dynamics CRM.
Tech.53	L'entrepreneur doit créer un processus qui permettra d'enregistrer les configurations antérieures de la solution pour appuyer le retour à une version antérieure pour une période qui sera définie par le GC.
Tech.54	L'entrepreneur doit configurer la solution pour prévenir le transfert d'information non autorisé et involontaire au moyen de ressources système partagées.
Tech.55	L'entrepreneur doit configurer la solution pour répondre automatiquement lorsque des infractions à l'intégrité se produisent.

PARTIE 4 : ACCÈS SÉCURISÉ

La présente section définit les exigences liées à l'accès sécurisé et à l'authentification des utilisateurs de la solution.

1.1 APERÇU DES EXIGENCES

L'entrepreneur doit assurer un accès sécurisé à deux grands groupes d'utilisateurs : les utilisateurs internes (p. ex., les employés du gouvernement) et les utilisateurs externes (p. ex., les demandeurs du Programme des marchandises contrôlées). Voir l'appendice 3 de l'annexe A pour plus de renseignements.

En ce qui concerne le groupe des utilisateurs internes, l'accès sécurisé que fournit l'entrepreneur doit interagir avec la solution de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA ou PasseGC) du GC, en particulier avec les divers aspects de la solution ayant trait à la gestion des justificatifs, notamment :

(a) la gestion des justificatifs d'identité des utilisateurs;
(b) le service d'authentification pour tous les renseignements;
(c) le soutien des signatures électroniques par la possibilité offerte à l'utilisateur de donner son consentement par voie électronique plutôt qu'au moyen d'une signature.

La gestion des justificatifs d'identité est prise en charge par Services partagés Canada (SPC). On l'appelle le service de gestion des justificatifs internes. Ce service est fondé sur la technologie d'infrastructure à clé publique (ICP) qu'on appelle maCLÉ. Le service maCLÉ est actuellement utilisé à TPSGC (et offert à l'échelle du GC) aux fins d'authentification des employés pour accéder à divers systèmes du GC nécessitant des contrôles d'accès accrus. Pour mieux répondre aux besoins du GC en matière de sécurité, le Conseil du Conseil du Trésor effectue la migration de "maCLÉ" a PasseGC.

En ce qui concerne le groupe des utilisateurs externes, l'accès sécurisé que fournit l'entrepreneur doit interagir avec les éléments suivants :

(a) la cléGC, un justificatif électronique offert aux personnes de l'extérieur et soutenu par le GC;
(b) Secure-Key Concierge (ou Partenaires de Connexion) est un partenariat établi entre les grands établissements bancaires canadiens et le Canada.

1.2 EXIGENCES DÉTAILLÉES

1.2.1 Utilisateurs internes

L'entrepreneur doit mettre en œuvre une solution qui réponde, sans pour autant s'y limiter, aux exigences énumérées ci-dessous.

Section de l'EDT	Exigence
SécurInt.01	S'intégrer au service d'authentification maCLÉ qu'assure SPC.
SécurInt.02	Assurer l'authentification de l'utilisateur au moyen du service maCLÉ et d'une deuxième méthode (par exemple, les secrets partagés) à l'ouverture d'une session dans la solution.

Section de l'EDT	Exigence
SécurInt.03	Respecter le protocole allégé d'accès annuaire (LDAP)
SécurInt.04	Relier un justificatif maCLÉ à un compte d'utilisateur correspondant.
SécurInt.05	Limiter, par rôle d'utilisateur, le nombre de connexions simultanées admissibles à la solution pour un même compte d'utilisateur, conformément à la norme de sécurité (ITSG-33 AC-10).
SécurInt.06	Faire en sorte que l'utilisateur puisse accéder au Système partagé de gestion des cas (SPGC) au moyen d'un réseau privé virtuel (RPV).
SécurInt.07	Utilise des signatures numériques pour les processus liés aux utilisateurs internes, au besoin.

1.2.2 Utilisateurs externes

L'entrepreneur doit mettre en œuvre une solution qui réponde, sans pour autant s'y limiter, aux exigences énumérées ci-dessous.

Section de l'EDT	Exigence
SécurExt.01	S'intégrer à cléGC et à Secure-Key Concierge.
SécurExt.02	Assurer l'authentification de l'utilisateur au moyen de cléGC ou de Secure-Key Concierge et d'une deuxième méthode (par exemple, les secrets partagés) à l'ouverture d'une session dans le service vertical web initial destinées au public de la solution.
SécurExt.03	Relier un justificatif cléGC ou Secure-Key Concierge à un compte d'utilisateur correspondant.
SécurExt.04	Limiter, par rôle d'utilisateur, le nombre de connexions simultanées admissibles à la solution pour un même compte d'utilisateur, conformément à la norme de sécurité (ITSG-33 AC-10).
SécurExt.05	Satisfaire aux exigences du SCT en matière de cyber authentification et permettre s'il y a lieu l'utilisation des jetons d'authentification de niveau LoA2 et LoA3 en s'appuyant sur les conseils que donne le CSTC dans sa publication « CSTC, ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI », version 2.

PARTIE 5 : EXIGENCES RELATIVES À LA SÉCURITÉ DE LA TI

La présente partie définit les exigences liées à la sécurité auxquelles doit satisfaire la solution.

1.1 APERÇU DES EXIGENCES

1.1.1 Processus d'évaluation de la sécurité et d'autorisation

Le GC a beaucoup investi dans les systèmes de TI et souhaite protéger le plus étroitement possible les biens issus de ses activités. En vue d'atteindre cet objectif, il s'est doté d'un processus solide d'évaluation de la sécurité et d'autorisation (ESA). Au cours de son développement, chaque système d'information doit franchir plusieurs points de contrôle avant d'être lancé dans l'environnement de production. Le tableau qui suit présente les exigences de haut niveau associées à ces divers points de contrôle, et les exigences détaillées figurent dans la sous-section du même nom.

Point de contrôle ESA	Exigence
ESA.01	L'entrepreneur doit réaliser : (a) la conception générale d'une solution en matière de sécurité; (b) la matrice de traçabilité des exigences relatives à la sécurité.
ESA.02	Par suite de l'acceptation des travaux associés au premier point de contrôle d'ESA, et sous réserve de l'approbation du responsable de projet, l'entrepreneur doit réaliser : (a) la conception détaillée des composants de sécurité se rattachant à la solution; (b) mise à jour de la matrice de traçabilité des exigences relatives à la sécurité. (c) les procédures de gestion du changement; (d) les procédures opérationnelles de sécurité; (e) les procédures d'installation des composants de sécurité.
ESA.03	Par suite de l'acceptation des travaux associés au second point de contrôle d'ESA, et sous réserve de l'approbation du responsable de projet, l'entrepreneur doit établir : (a) un plan de vérification de l'installation des composants de sécurité; (b) un rapport de vérification de l'installation des composants de sécurité; (c) un plan relatif aux essais d'intégration de la sécurité; (d) un rapport relatif aux essais d'intégration de la sécurité; (e) une matrice de traçabilité des exigences relatives à la sécurité à jour comprenant une mise en correspondance du rapport relatif aux essais d'intégration de la sécurité avec les exigences en matière de sécurité; (f) un plan d'évaluation de la vulnérabilité; (g) une matrice de traçabilité des exigences relatives à la sécurité à jour comprenant une mise en correspondance du rapport d'évaluation des vulnérabilités avec les exigences en matière de sécurité.

1.1.2 Catalogue des contrôles de sécurité

L'explication suivante fournit une description à très haut niveau du catalogue de sécurité de la technologie de l'information 33 (ITSG-33), organisé par classes et contrôle de familles. Ces contrôles s'appliquent aux exigences de sécurité de SSI et par les exigences détaillées dans L'ANNEXE. Puisque la solution complète sera essentiellement un exercice d'intégration, la suite complète des contrôles sera évaluée tout au long du développement de la solution en utilisant le processus d'évaluation et d'autorisation de sécurité. Ces contrôles sont à la base de la sécurisation de la solution et de ses données.1.1.2.1 Classe de contrôles de sécurité techniques

La classe de contrôles de sécurité techniques comprend les familles de contrôle définies ci-dessous.

(a) Contrôle d'accès : contrôles de sécurité permettant d'autoriser ou d'interdire à un utilisateur l'accès aux ressources contenues dans un système d'information.
(b) Vérification et responsabilité : contrôles de sécurité permettant de recueillir, d'analyser et de stocker des rapports de vérification liés aux interventions de l'utilisateur dans le système d'information.
(c) Identification et authentification : contrôles de sécurité permettant de vérifier l'identification et l'authentification uniques des utilisateurs lorsqu'ils tentent d'accéder aux ressources du système d'information.
(d) Protection du système et des communications : contrôles de sécurité permettant de protéger le système d'information lui-même, ainsi que ses communications internes et externes.

1.1.2.2 Classe de contrôles de sécurité opérationnels

La classe de contrôles de sécurité opérationnels comprend les familles de contrôle définies ci-dessous.

(a) Sensibilisation et formation : contrôles de sécurité qui se rapportent à la formation des utilisateurs quant à la sécurité du système d'information.
(b) Gestion de la configuration : contrôles de sécurité facilitant la gestion et l'administration de tous les composants du système d'information (p. ex. matériel, logiciel et éléments de configuration).
(c) Planification d'urgence : contrôles de sécurité permettant l'accès aux services du système d'information en cas de défaillance d'un composant ou de sinistre.
(d) Intervention en cas d'incident : contrôles de sécurité appuyant la détection des incidents en matière de sécurité survenus dans le système d'information, la réaction à ces incidents et l'établissement de rapports d'incidents.
(e) Maintenance : contrôles de sécurité facilitant l'entretien du système d'information en vue d'en assurer la disponibilité à long terme.
(f) Protection des supports : contrôles de sécurité permettant de protéger les supports du système d'information (disques, bandes magnétiques, etc.) tout au long de leur cycle de vie.
(g) Protection physique et environnementale : contrôles de sécurité liés à l'accès physique à un système d'information et à la protection de l'équipement environnemental auxiliaire (électricité, climatisation, câblage, etc.) servant à l'exploitation du système d'information.
(h) Sécurité du personnel : contrôles de sécurité servant à appliquer les procédures nécessaires pour veiller à ce que tous les membres du personnel ayant accès au système d'information détiennent les autorisations de sécurité requises.
(i) Intégrité du système et de l'information : contrôles de sécurité permettant de protéger l'intégrité des composants du système d'information et des données traitées par ce système.

1.1.2.3 Classe de contrôles de sécurité

La classe de contrôles de sécurité de gestion comprend les familles de contrôle définies ci-dessous.

(a) Évaluation et autorisation de sécurité : contrôles de sécurité du système d'information liés à l'évaluation de la sécurité et à l'autorisation.
(b) Planification : contrôles de sécurité liés aux activités de planification de la sécurité, y compris l' évaluation des facteurs relatifs à la protection des renseignements personnels.
(c) Évaluation des risques : contrôles de sécurité liés à la réalisation de l'évaluation des risques et à l'analyse de la vulnérabilité.
(d) Acquisition des systèmes et des services : contrôles de sécurité liés à la passation de marchés pour l'acquisition de produits et de services nécessaires à la mise en œuvre et à l'exploitation du système d'information.

1.2 EXIGENCES DÉTAILLÉES

Le tableau si dessous établisse les exigences de sécurité qui viennent des contrôles du ITSG-33 et qui sont la responsabilité de l'entrepreneur. Les exigences présentées ici sont exclus par les éléments dont on s'attend à ce qu'ils soient pris en charge par TPSGC comme organisation au moyen des implémentations technologiques existantes. Ça sera la responsabilité de l'entrepreneur d'intégrer tous les contrôles de sécurité, y compris ceux rencontrés par TPSGC, SSC et l'entrepreneur dans la matrice de traçabilité des exigences relatives à la sécurité.L'entrepreneur doit mettre en œuvre une solution qui réponde, sans pour autant s'y limiter, aux exigences en matière de sécurité de la TI énumérées ci-dessous.

Catégorie	Section de l'EDT	Exigence
Contrôle d'accès et gestion des comptes	SC.00.A	L'entrepreneur doit préparer un plan de contrôle de l'accès et de gestion des utilisateurs
	SC.01	La solution doit : (a) imposer à chaque utilisateur des contrôles d'accès fondés sur le rôle; (b) répartir les utilisateurs selon des rôles établis suivant le principe du « droit d'accès minimal » et du « besoin de connaître »; (c) désactiver automatiquement les comptes inactifs ou inutilisés après une période déterminée par les impératifs opérationnels; (d) créer des journaux de vérification sur la création, la modification, le retrait, l'activation et la désactivation des comptes; (e) fermer ou verrouiller la session de l'utilisateur et dissimuler les renseignements affichés après une période d'inactivité pertinente, conformément aux politiques du GC et aux pratiques exemplaires de l'industrie; (f) garder la session verrouillée jusqu'à ce que l'utilisateur rétablisse l'accès en recourant aux procédures d'identification et d'authentification établies; (g) attribuer la création d'un compte à un utilisateur unique, particulier; (h) exiger l'utilisation de comptes ou de rôles non privilégiés pour l'accès aux fonctions qui ne sont pas liées à la sécurité; (i) limiter le nombre de tentatives d'ouverture de session infructueuses avant de verrouiller le compte;

Catégorie	Section de l'EDT	Exigence
		(j) informer l'utilisateur de la dernière ouverture de session réussie en incluant la date et l'heure, ainsi que le nombre de tentatives d'ouverture de session infructueuses ayant précédé la dernière ouverture de session réussie; (k) informer l'utilisateur de toute modification apportée aux rôles et aux droits se rattachant à son compte depuis la dernière ouverture de session réussie; (l) offrir les fonctions permettant aux personnes autorisées de configurer, de définir, de modifier et d'afficher les caractéristiques de sécurité de l'information stockée, en traitement ou en cours de transmission; (m) offrir la fonction permettant d'afficher une bannière d'ouverture de session.
	SC.02	L'entrepreneur doit consigner les rôles et les responsabilités, les caractéristiques et les capacités des entrepreneurs, des employés et des tiers utilisateurs en ce qui a trait à la sécurité et aux ressources d'information de la solution du SSI de TPSGC.
	SC.03	L'entrepreneur doit au besoin veiller à la séparation des tâches des utilisateurs afin d'éviter toute activité malveillante et toute collusion en fonction du profil d'accès accordé à l'utilisateur selon son rôle.
Vérification et responsabilisation	SC.04	La solution doit : (a) générer, suivant un format normalisé, des journaux de vérification contenant, à tout le moins, des renseignements établissant le type d'événement qui s'est produit, le moment, le lieu, la source et l'issue de l'événement, ainsi que l'identité de toute personne associée à l'événement ou tout sujet qui s'y rattache; (b) offrir la fonction permettant de configurer des avertissements et des alertes suivant les différents états de la vérification (p. ex., si le journal de vérification a atteint une capacité de stockage maximale, ou si d'autres défaillances se produisent); (c) générer des journaux de vérification liés aux incidents suivant un format permettant la transmission à un système de gestion de l'information et des incidents concernant la sécurité (GIIS); (d) effectuer l'horodatage des journaux de vérification en utilisant une source exacte.
	SC.05	L'entrepreneur doit étayer le contenu et le format des journaux de vérification relatifs à la sécurité, et fournir des estimations pertinentes quant aux exigences relatives au stockage et à la bande passante en vue d'assurer la gestion de ces journaux. La documentation doit en outre établir clairement leur caractère prioritaire ou leur importance afin de permettre la formulation de règles liées aux alertes et à la surveillance.
	SC.06	La solution doit : (a) protéger les renseignements de vérification contre l'accès, les modifications et la suppression non autorisés; (b) sauvegarder les dossiers de vérification dans un système ou un support différent de celui dont la vérification est prévu au calendrier selon les

Catégorie	Section de l'EDT	Exigence
		directives de TPSGC.
Identification et authentification	SC.07	La solution doit : (a) identifier et authentifier de façon unique les utilisateurs; (b) comporter des mécanismes d'authentification conformes aux exigences et aux lignes directrices du Centre de la sécurité des télécommunications (CSTC), aux politiques du Secrétariat du Conseil du Trésor du Canada (SCT), ainsi qu'aux pratiques exemplaires.
	SC.08	La solution doit : (a) permettre l'authentification mutuelle des connexions entre la solution et les autres domaines, selon les directives de TPSGC, et autoriser exclusivement les échanges d'information avec ces autres domaines en utilisant l'authentification mutuelle; (b) garantir que l'intégrité et la confidentialité des données, durant la transmission et en période d'arrêt, sont protégées à l'aide de solutions cryptographiques, sauf si elles sont protégées par d'autres mécanismes approuvés par TPSGC; (c) suivre les conseils en matière de sécurité des TI des documents ITSG-22 et ITSG-38.
Connexions au système d'information	SC.09	L'entrepreneur doit : (a) documenter rigoureusement tous les liens existant entre les systèmes de TI, notamment la description des données, le flux de données, les exigences et les mécanismes liés à la sécurité et à l'accès, le rendement, les attentes touchant la fiabilité, etc. (b) fournir la preuve que les fournisseurs de services informatiques externes se conforment aux exigences de contrôle de la sécurité informatique de l'organisation et utilisent des contrôles de sécurité conformément à la Norme de sécurité et de gestion des marchés du SCT.
Gestion des configurations	SC.10	L'entrepreneur doit consigner dans son intégralité la configuration de base de la solution, conformément aux exigences.
	SC.11	L'entrepreneur doit évaluer l'incidence des changements sur la sécurité s'il procède à la mise en œuvre de nouveaux logiciels, à un important changement de configuration ou à la gestion des correctifs. Son évaluation comportera les points suivants : (a) analyse des nouveaux logiciels avant leur installation dans un environnement opérationnel afin de déterminer les répercussions sur la sécurité attribuables aux failles, aux points faibles, à l'incompatibilité ou à la malveillance intentionnelle; (b) communication à TPSGC de l'incidence possible sur la sécurité des changements avant leur mise en œuvre; (c) vérification des fonctions de sécurité après les changements pour s'assurer qu'elles ont été mises en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités quant au respect des exigences pertinentes

Catégorie	Section de l'EDT	Exigence
		en matière de sécurité.
	SC.12	L'entrepreneur doit permettre uniquement l'exécution des logiciels autorisés qu'il a lui-même établis et qui ont obtenu l'approbation de TPSGC, dans le cadre de la solution.
	SC.13	L'entrepreneur doit utiliser des mécanismes automatisés afin de gérer, d'appliquer et de vérifier les paramètres de configuration de façon centrale et de réagir aux changements non autorisés apportés à la configuration en créant un dossier d'incident de sécurité (envoyer à : DGDPI OPERATIONS GI TI / CIOB IM IT OPERATIONS (TPSGC/PWGSC) TPSGC.dgdpioperationsgiti-ciobimitoperations.PWGSC@tpsgc-pwgsc.gc.ca
	SC.14	L'entrepreneur doit suivre le processus de gestion des demandes de changement de TPSGC lorsqu'il souhaite apporter un changement à la solution.
Planification d'urgence	SC.15	L'entrepreneur doit consigner le plan d'urgence dans son intégralité pour faire en sorte que les divers secteurs d'activités du SSI répondent en tout temps aux exigences minimales de la planification d'urgence pour PB/H/M.
Architecture de sécurité de l'information	SC.16	L'entrepreneur doit, dans le cadre de la solution, consigner l'architecture de sécurité de l'information en respectant les paramètres suivants : (a) décrire globalement la philosophie, les exigences et l'approche qu'il prévoit adopter relativement à l'information afin d'assurer la confidentialité, l'intégrité et l'accès; (b) décrire la façon dont il assurera l'intégration et le soutien de l'architecture de sécurité de l'information à l'architecture d'entreprise; (c) décrire toute hypothèse relative à la sécurité de l'information qui porterait sur les services externes et tout lien de dépendance à l'égard de ceux-ci.
	SC.17	L'entrepreneur doit fournir la conception générale d'une solution en matière de sécurité qui comporte à tout le moins : (a) un schéma général des composants qui illustre clairement la répartition des services et des composants dans les zones de sécurité du réseau et qui établit les principaux flux de données liés à la sécurité; (b) les couches de l'architecture (p. ex. communication, virtualisation, plateforme/système d'exploitation, gestion des données, intergiciels, applications opérationnelles); (c) une description des mesures de défense du périmètre de la zone du réseau; (d) une description de l'utilisation des technologies de virtualisation, s'il y a lieu; (e) une description de la répartition de l'ensemble des exigences de sécurité technique dans les éléments de la conception générale des services, et ce, pour toutes les couches de l'architecture; (f) une description de la répartition de l'ensemble des exigences de sécurité non technique au sein des éléments organisationnels ou opérationnels généraux; (g) une description de l'approche relativement à : i. la gestion à distance;

Catégorie	Section de l'EDT	Exigence
		ii. le contrôle d'accès; iii. la gestion et la vérification de la sécurité; iv. la gestion de la configuration; v. la gestion des correctifs. (h) une justification des principales décisions concernant la conception.
	SC.18	(a) L'entrepreneur doit fournir la conception détaillée d'une solution en matière de sécurité qui comporte à tout le moins :un schéma détaillé des composants (il doit s'agir d'une version approfondie du schéma général des composants); (b) une description de la répartition des mécanismes de sécurité technique au sein des éléments de la conception détaillée des services; (c) la description de l'association des mécanismes de sécurité non technique aux éléments de la conception générale qui concernent l'organisation ou les opérations; (d) une justification des principales décisions concernant la conception.
Protection des limites	SC.19	La solution doit : (a) être mise en œuvre de manière à résister aux attaques entraînant un refus de service afin d'atteindre la disponibilité cible du SSI; (b) comporter des dispositifs de surveillance et de contrôle à ses limites extérieures (connexions Internet et GC); (c) être configurée de manière à refuser la communication par défaut et à ne permettre que les communications autorisées; (d) pouvoir détecter et refuser les communications qui semblent constituer une menace pour les systèmes internes et externes, et attribuer ces communications à une personne dans toute la mesure du possible; (e) protéger l'authenticité des sessions de communication; (f) annuler les identifiants de session lors de la fermeture de la session ou de tout autre type de déconnexion; (g) utiliser des identificateurs de session unique et ne reconnaître que les identificateurs générés par le système.
	SC.20	La solution doit s'interrompre par mesure préventive en cas de défaillance des dispositifs de protection des limites.
Protection de l'information	SC.21	La solution doit : (a) protéger l'information en transit entre les systèmes; (b) protéger l'information inactive à l'intérieur du système; (c) comporter une fonction permettant d'intégrer des solutions cryptographiques, conformément aux recommandations du CSTC et aux politiques du SCT.
Code mobile et programme malveillant	SC.22	La solution doit : (a) employer, aux points d'entrée et de sortie de la solution, des mécanismes de protection capables de détecter et d'éliminer les programmes malveillants; (b) tenir à jour les mécanismes de protection contre les programmes malveillants, conformément aux politiques organisationnelles relatives à la gestion de la configuration;

Catégorie	Section de l'EDT	Exigence
		(c) utiliser un code mobile uniquement si toute la démarche se trouve rigoureusement consignée et conserver les autres dispositifs de protection de la solution.
Surveillance du système d'information	SC.23	La solution doit : (a) pouvoir détecter les attaques, les indicateurs d'attaques potentielles, ainsi que les réseaux locaux et les connexions à distance non autorisés; (b) informer les administrateurs de la sécurité de ces détections.
Caractéristiques de sécurité	SC.24	La solution doit permettre aux utilisateurs privilégiés de définir ou de modifier la valeur des caractéristiques de sécurité des objets.
Fonctionnalité minimale	SC.25	La solution doit être configurée selon les pratiques exemplaires de l'industrie et les politiques du GC relatives au renforcement de la sécurité des systèmes d'information, ce qui comprend, sans pour autant s'y limiter, la désactivation des ports, protocoles et services inutiles.
	SC.26	L'entrepreneur doit consigner chacun des ports et des protocoles nécessaires à la solution. Ce document doit comprendre à tout le moins : (a) le port, le protocole ou le service utilisé; (b) une description de l'information transférée dans ce port, ce protocole ou ce service; (c) une description du flux (source et destination); (d) les règles relatives au pare-feu ou à l'acheminement nécessaires au soutien de la communication.
Mise à l'essai des mécanismes de sécurité	SC.27	L'entrepreneur doit : (a) établir et mettre en œuvre un plan d'évaluation de la sécurité; (b) produire la preuve de l'exécution du plan d'évaluation de la sécurité, ainsi que les résultats de la mise à l'essai ou de l'évaluation des mécanismes de sécurité; (c) mettre en œuvre un processus vérifiable de correction des failles; (d) corriger les failles repérées au cours de la mise à l'essai ou de l'évaluation des mécanismes de sécurité. Avant de recevoir l'autorisation d'être mise en place dans un environnement de production, la solution doit faire l'objet d'une analyse des vulnérabilités réalisée à l'aide des outils normalisés de l'industrie, et les vulnérabilités repérées doivent être corrigées à la satisfaction de TPSGC.
Récupération et reconstitution du système d'information	SC.28	L'entrepreneur doit consigner toutes les procédures relatives à la récupération et à la Reconstitution de la solution, conformément aux exigences minimales pour PB/H/M.
Composants du système non pris	SC.29	L'entrepreneur doit consigner un plan d'entretien et de soutien des composants et sous-composants de la solution : celle-ci ne doit pas faire l'objet d'un soutien réduit en

Catégorie	Section de l'EDT	Exigence
en charge		raison d'un appui insuffisant des sous-composants, ou présenter des vulnérabilités qui ne sont pas corrigées à cause de ces sous-composants.
Création et gestion des clés cryptographiques	SC.30	La solution doit créer et gérer les clés cryptographiques conformément aux lignes directrices établies par le CSTC.
Validation de la saisie des données	SC.31	La solution doit vérifier la validité des données saisies.
Gestion des incidents	SC.32	L'entrepreneur doit, pour la durée du contrat, apporter son aide au GC et intervenir en cas d'incident présumé ou réel lié à la solution.
	SC.33	L'entrepreneur doit, pour la durée du contrat, signaler au nombre des incidents toute atteinte présumée ou réelle à la vie privée et à la sécurité.
	SC.34	L'entrepreneur doit, pour la durée du contrat, apporter son appui et son aide au GC avec la mise en œuvre des mesures d'atténuation (p. ex. blocage à l'aide du pare-feu, signatures personnalisées des services de détection et de prévention d'intrusion, suppression des logiciels malveillants) afin de maîtriser un incident de sécurité, d'assurer une protection contre les cybermenaces et d'éliminer les vulnérabilités, à la demande des représentants autorisés de TPSGC, selon les directives du Ministère et conformément au niveau de priorité du Canada.
	SC.35	L'entrepreneur doit apporter son appui et son aide au GC à l'établissement d'un plan d'intervention.
	SC.36	L'entrepreneur doit, pour la durée du contrat, apporter son appui et son aide à la préparation d'un rapport rétrospectif sur l'incident de sécurité, à la demande de TPSGC.
	SC.37	L'entrepreneur doit, pour la durée du contrat, créer un ou plusieurs dossiers d'incident pour chaque incident relevé.
Surveillance continue	SC.38	L'entrepreneur doit, pour la durée du contrat, apporter son appui et son aide au GC pour le maintien du niveau de sécurité de la solution en s'employant constamment à relever les problèmes suivants et à en informer le GC : (a) les menaces et les vulnérabilités; (b) les activités malveillantes et les accès non autorisés.
Évaluation des risques	SC.39	L'entrepreneur doit élaborer un plan d'atténuation des vulnérabilités de la solution approuvé par TPSGC dans les cinq jours ouvrables suivant l'achèvement d'une évaluation de la vulnérabilité : le plan propose des mesures de protection pour atténuer les risques ciblés dans cette évaluation.
	SC.40	L'entrepreneur doit, pour la durée du contrat, installer des correctifs ou mettre en

Catégorie	Section de l'EDT	Exigence
		œuvre des mesures correctives dans le cadre de l'évaluation de la vulnérabilité. L'entrepreneur doit créer un dossier de demande de service pour les correctifs ou les mesures correctives qui ne peuvent être mis en œuvre dans le cadre de l'évaluation de la vulnérabilité.
Sécurité – Généralités	SC.41	La solution doit, à tout le moins, satisfaire aux exigences pour PB/H/M.
	SC.42	L'entrepreneur doit présenter au GC, aux fins d'approbation, un plan relatif aux essais d'intégration de la sécurité qui accompagnera le plan de sécurité des TI. Ce plan relatif aux essais d'intégration doit à tout le moins comprendre : (a) les fonctions de sécurité faisant l'objet d'essais; (b) les dispositions nécessaires pour permettre au GC d'assister aux essais; (c) pour chaque fonction de sécurité ou ensemble de fonctions de sécurité, les éléments qui seront mis à l'essai, y compris : i. la description de chaque scénario et procédure d'essai; ii. les exigences en matière d'environnement; iii. les liens de dépendance; iv. les résultats attendus (c.-à-d. des critères de type réussite/échec).
	SC.43	La solution doit maintenir l'intégrité des données durant leur conversion aux divers protocoles et formats de données**.**
	SC.44	La solution doit faire appliquer les autorisations approuvées pour contrôler la circulation de l'information dans le système et entre des systèmes interreliés.
	SC.45	L'entrepreneur doit obtenir l'approbation de TPSGC pour l'utilisation de systèmes d'information externes (c.-à-d. des systèmes n'appartenant pas à l'entrepreneur) en vue de la mise en œuvre de la solution.
Généralités	SC.46	L'entrepreneur doit obtenir l'approbation de TPSGC avant de mettre le contenu relatif à la solution à la disposition du public.
	SC.47	L'entrepreneur doit présenter au GC des procédures opérationnelles de sécurité. Celles-ci doivent à tout le moins comprendre les éléments énumérés ci-dessous. (a) Pour chaque rôle d'utilisateur privilégié : i. un calendrier des mesures liées à la sécurité qui doivent être prises pour maintenir le niveau de sécurité du SSI; ii. la façon d'utiliser les interfaces opérationnelles en fonction; iii. chaque mesure prévue et la façon dont l'utilisateur doit l'appliquer. (b) Les rôles et responsabilités opérationnels concernant : i. les exigences relatives à l'interaction avec les représentants de TPSGC; ii. l'échéancier et les procédures d'établissement de rapports; iii. le contrôle d'accès; iv. la vérification et la responsabilisation; v. l'identification et l'authentification; vi. la protection du système et des communications; vii. la sensibilisation et la formation; viii. la gestion de la configuration;

Catégorie	Section de l'EDT	Exigence
		ix. la planification d'urgence; x. l'intervention en cas d'incident; xi. l'entretien; xii. la protection des supports d'information; xiii. la protection physique et environnementale; xiv. la sécurité du personnel; xv. l'intégrité du système et de l'information.
	SC.48	L'entrepreneur doit présenter au GC des procédures détaillées d'installation des composants de sécurité. Celles-ci doivent à tous le moins comprendre : (a) les étapes nécessaires à l'installation et à la configuration sécurisées; (b) l'installation et la configuration de l'ensemble des solutions de sécurité technique; (c) la configuration des composants de sécurité des produits matériels; (d) la configuration de la sécurité des produits logiciels.
	SC.49	L'entrepreneur doit présenter au GC un plan de vérification et un rapport de vérification de l'installation des composants de sécurité. Ce plan doit à tout le moins comprendre : (a) l'approche adoptée pour vérifier la sécurité; (b) les dispositions nécessaires pour permettre au GC d'assister aux essais; (c) un aperçu des composants faisant l'objet d'une vérification de la sécurité; (d) pour chacun des composants de sécurité vérifiés : i. une description du scénario de vérification; ii. les liens de dépendance; iii. les résultats attendus (c.-à-d. des critères de type réussite/échec); iv. Résultats actuels; v. Une description de l'écart et comment chacun a été résolu.
	SC.50	L'entrepreneur doit, pour la durée du contrat, apporter son soutien et son aide au GC pour effectuer une vérification de l'installation des composants de sécurité conformément au plan de vérification de l'installation des composants de sécurité approuvé.
	SC.51	L'entrepreneur doit corriger les erreurs et omissions ayant trait à l'installation ou à la configuration relevées dans le cadre de la vérification de l'installation des composants de sécurité.
	SC.52	L'entrepreneur doit effectuer des essais d'intégration de la sécurité conformément au plan relatif aux essais d'intégration de la sécurité.
	SC.53	L'entrepreneur doit fournir un rapport relatif aux essais d'intégration de la sécurité qui comprend, à tout le moins, pour chacun des éléments mis à l'essai dans le cadre du plan : (a) les résultats attendus (c.-à-d. des critères de type réussite/échec); (b) les résultats obtenus; (c) une description des écarts et la méthode employée pour corriger ces derniers.

Catégorie	Section de l'EDT	Exigence
	SC.54	L'entrepreneur doit utiliser de l'information non sensible ou des techniques de masquage des données afin de remplacer l'information sensible dans les environnements qui ne sont pas liés à la production.
	SC.55	L'entrepreneur doit, durant tout le processus d'évaluation de la sécurité et d'autorisation, tenir à jour à l'intention du GC une matrice de traçabilité des exigences relatives à la sécurité. Celle-ci doit à tout le moins comprendre : (a) un code d'identification des exigences en matière de sécurité; (b) un identifiant qui met en correspondance l'exigence en matière de sécurité et l'élément correspondant dans l'EDT (p. ex. identificateur d'en-tête ou de ligne); (c) un énoncé des exigences en matière de sécurité; (d) une description suffisamment détaillée de la façon dont on répond aux exigences dans la conception – générale et détaillée – d'une solution en matière de sécurité, pour permettre au GC de confirmer que les mesures de sécurité satisfont aux exigences à cet égard; (e) le titre du ou des produits livrables associés au contrat dans lesquels l'entrepreneur présentera les détails de la solution de sécurité qu'il entend adopter pour répondre à l'exigence (p. ex. plan de continuité des services); (f) la traçabilité (une référence à un élément identifiable) de la conception – générale et détaillée – d'une solution en matière de sécurité, pour permettre au GC de confirmer que les mesures de sécurité satisfont aux exigences à cet égard; (g) pour chaque exigence en matière de sécurité devant être mise à l'essai par l'intermédiaire du plan de vérification de l'installation des composants de sécurité, la traçabilité (une référence à un élément identifiable) des scénarios d'essai relatifs à la vérification de l'installation des composants de sécurité; (h) pour chaque exigence en matière de sécurité devant être mise à l'essai par l'intermédiaire du plan relatif aux essais d'intégration de la sécurité, la traçabilité (une référence à un élément identifiable) des scénarios d'essai relatifs aux essais d'intégration de la sécurité.
Gestion des comptes	SC.56	La solution doit créer des comptes d'utilisateur en s'appuyant sur les rôles approuvés par le GC.
Gestion des comptes et droits d'accès minimaux	SC.57	La solution doit effectuer la vérification des activités du compte d'utilisateur et des privilèges associés au compte, et créer un rapport fondé sur des critères à sélectionner.
Application des contrôles du flux d'information	SC.58	La solution ne doit accepter que la transmission des types de données approuvés par le GC.
	SC.59	La solution et la plateforme qui y est associée doivent analyser l'information – entrante et sortante – afin de détecter les programmes malveillants et les contenus inacceptables.

Catégorie	Section de l'EDT	Exigence
Contrôle des sessions simultanées	SC.60	La solution doit limiter le nombre de sessions simultanées des comptes privilégiés ou non privilégiés, ainsi que de tous les autres types de comptes, selon les indications du GC.
Fermeture de session	SC.61	La solution doit automatiquement mettre fin à la session après une période d'inactivité de l'utilisateur déterminée par le GC.
	SC.62	La solution doit : (a) fermer la session de communication amorcée par l'utilisateur si une authentification est utilisée; (b) afficher un message de fermeture de session clair pour indiquer à l'utilisateur que la session de communication authentifiée s'est terminée d'une façon fiable.
Caractéristiques de sécurité	SC.63	La solution doit comporter des mécanismes permettant de maintenir l'association et l'intégrité des caractéristiques de sécurité définies par le GC.
	SC.64	La solution doit mettre en œuvre des technologies ou des techniques convenant au niveau d'assurance établi par le GC en vue d'associer les caractéristiques de sécurité à l'information.
Protection contre l'exploration de données	SC.65	La solution doit employer des techniques de prévention et de détection pour contrer l'exploration des données, notamment : i) limiter les types de réponses fournies lors de l'interrogation de la base de données; ii) limiter le nombre ou la fréquence des interrogations de la base de données afin d'accroître les facteurs travail nécessaires pour déterminer le contenu de cette base de données; iii) informer le personnel de l'organisation lorsque des interrogations atypiques de la base de données ou des accès inhabituels se produisent relativement à des objets de stockage de données, par exemple les bases de données, les enregistrements de bases de données et les champs de bases de données. La solution assurera ainsi une détection et une protection appropriées contre l'exploration de données.
Protection des renseignements de vérification	SC.66	La solution doit mettre en œuvre des mécanismes de chiffrement pour protéger la confidentialité des renseignements et des outils liés à la vérification.
Non-répudiation	SC.67	La solution doit assurer une protection contre un individu (ou un processus exécuté au nom d'un individu) qui nie faussement avoir expédié ou reçu un document résultant d'un mouvement.
	SC.68	La solution doit : (a) lier l'identité du producteur d'information et l'information produite selon la force du lien établie par le GC; (b) fournir aux personnes autorisées le moyen de déterminer l'identité du producteur d'information.

Catégorie	Section de l'EDT	Exigence
	SC.69	La solution doit : (a) valider le lien entre l'identité du producteur d'information et l'information produite, suivant la fréquence établie par le GC; (b) exécuter les interventions définies par le GC en cas d'erreur de validation.
Identification et authentification (utilisateurs organisationnels)	SC.70	La solution doit mettre en œuvre l'authentification multifactorielle pour permettre au réseau d'accéder : (a) aux comptes privilégiés; (b) aux comptes non privilégiés.
Gestion des authentificateurs	SC.71	
Réauthentification	SC.72	La solution doit réauthentifier les utilisateurs et les appareils lorsque les authentificateurs, les rôles, les catégories de sécurité des systèmes d'information changent, en cas d'exécution de fonctions privilégiées, après une période prédéterminée, de façon périodique ou selon d'autres modalités établies par le GC.
Intégrité des logiciels, des micrologiciels et de l'information	SC.73	La solution doit mettre en œuvre des mécanismes de chiffrement pour éviter la divulgation non autorisée des renseignements et détecter les changements apportés aux logiciels, aux micrologiciels et à l'information.
Filtrage des sorties de données	SC.74	La solution doit valider les sorties de données des divers composants du SSI pour faire en sorte que ces données correspondent au contenu attendu.
Contrôle d'accès et gestion des comptes	SC.75	Lors de la création de documents de fonctionnement pour l'activité, l'entrepreneur devra inclure le ou les processus qui décrivent la gestion des rôles et des contrôles d'accès de l'utilisateur. Ces processus doivent être consignés par l'entrepreneur dans un plan de gestion et de contrôle de l'accès des utilisateurs et peuvent servir de preuves de l'évaluation et de l'autorisation de sécurité.

PARTIE 6 : GESTION DES ESSAIS

La présente partie définit les exigences liées aux essais auxquelles doit satisfaire la solution.

1.1 APERÇU DES EXIGENCES

À titre de principe directeur, l'entrepreneur doit exécuter tous les essais exigés de façon complète, exhaustive, non limitative, récurrente et opportune. L'entrepreneur doit s'assurer que les méthodes utilisées comprennent des processus d'assurance de la qualité, et cela, de l'étape de la conception à celle de la configuration, puis de la mise à l'essai. Ces processus d'assurance de la qualité :

(a) favoriseront la production hâtive de meilleurs plans d'essais;
(b) laisseront aux employés chargés des essais le temps de comprendre la solution;
(c) permettront d'effectuer les essais correctement dès le début;
(d) valideront chaque étape et chaque composant avant de poursuivre;
(e) amélioreront la qualité des spécifications et de la conception grâce à la rétroaction que susciteront la planification et la conception soignées des essais.

L'entrepreneur doit d'abord élaborer et tenir à jour le plan d'essai de la solution à chacune des étapes du développement : il actualisera le document à mesure que se préciseront les processus opérationnels afin de créer les scripts d'essai appropriés. On s'attend à ce qu'il utilise une ou plusieurs techniques – analyse fonctionnelle, équivalence, analyse de dépendance, analyse des valeurs limites, scénario utilisateur, listes de contrôle, analyse des risques ou autre – pour mener les essais. Ceux-ci seront de diverse nature : unitaires, de système, fonctionnels, de bout en bout, de sécurité (l'évaluation de la vulnérabilité sera menée par SPC et TPSGC), acceptation des clients, cycles d'essais. Dans le plan d'essai, l'entrepreneur doit décrire de façon détaillée les processus qui seront utilisés.

On fournira à l'entrepreneur des environnements de développement appropriés dans lesquels il pourra configurer les processus opérationnels approuvés avant de procéder aux essais.

L'entrepreneur doit, durant toute la période du contrat, gérer les travaux liés aux essais, ce qui inclut à tout le moins les activités énumérées ci-dessous.

(a) Élaborer un plan d'essai de base qui sera mis à jour à mesure qu'évolue la conception de la solution.
(b) Créer un cadre de gestion des défauts qui doit comprendre :
    i. le recours à un outil de suivi des défauts qui signale à l'équipe de projet les problèmes, leur incidence et leur résolution;
    ii. une échelle de gravité relative aux défauts;
    iii. des réunions de l'équipe chargée de la mise à l'essai au besoin du chargé de projet;
    iv. des rencontres régulières entre l'entrepreneur et le chargé de projet.
(c) Mettre à l'essai la documentation, notamment :
    i. les critères d'entrée et de sortie du test;
    ii. les jeux d'essai et les scripts d'essai;
    iii. les critères d'acceptation.
(d) Informer le responsable de la gestion des risques liés au projet de tout échec ou problème survenu au cours des essais.

1.2 EXIGENCES DÉTAILLÉES

L'entrepreneur doit répondre, sans pour autant s'y limiter, aux exigences relatives aux essais énumérées dans le tableau ci-dessous.

Catégorie	Section de l'EDT	Exigence
Gestion des essais (généralités)	TM.00.A	Préparer un plan d'essai préliminaire conformément aux exigences précisées à la section 6 de l'ANNEXE A. Le soumissionnaire devrait se fonder sur les exigences opérationnelles et techniques et l'architecture conceptuelle pour élaborer le plan d'essai.
	TM.01.A	Avant d'amorcer les travaux de développement, l'entrepreneur doit élaborer la stratégie de la mise à essai. Sous réserve de l'approbation du chargé de projet, la stratégie doit comprendre à tout le moins les renseignements suivants pour chacune des étapes des essais exigés : (a) un aperçu général de la stratégie proposée en ce qui a trait aux essais; (b) un cadre de gestion des défauts; (c) une stratégie d'entrée et de sortie; (d) des rencontres entre le chargé de projet et l'entrepreneur; (e) une stratégie permanente de gestion et d'atténuation des risques.
	TM.01.B	L'entrepreneur doit développer un de mise à l'essai qui doit démontrer à tout le moins : A. une prise en considération des exigences en matière de sécurité du Plan d'essai de l'intégration de la sécurité, SC-42, ainsi que de la section 6 de l'ANNEXE A; B. une couverture adéquate des essais pour s'assurer que les exigences clés atteignent l'état de production nécessaire. Prise en considération des points suivants et renvoi à ces derniers : i. un essai d'intégration; ii. des essais fonctionnels et non fonctionnels, notamment les essais de sécurité; iii. des essais de migration des données; iv. un essai d'acceptation par le client. C. La détection et gestion des risques.
	TM.02	L'entrepreneur doit, pour chaque étape de la mise à l'essai, élaborer des scripts convenant à la technique d'essai utilisée.
	TM.03	L'entrepreneur doit établir et tenir à jour le rapport de suivi des défauts durant toutes les étapes de la mise à l'essai. Le rapport doit à tout le moins contenir les renseignements suivants : (a) un registre constant de tous les défauts relevés durant la mise à l'essai de la solution; (b) la description des défauts, leur degré de gravité, l'étape de la mise à l'essai

Catégorie	Section de l'EDT	Exigence
		durant laquelle ils ont été découverts, les mesures prises pour les corriger et leur état actuel. L'entrepreneur doit transmettre le rapport au chargé de projet si ce dernier lui en fait la demande.
	TM.04	L'entrepreneur doit établir et tenir à jour le rapport d'avancement hebdomadaire durant toutes les étapes de la mise à l'essai. Le rapport doit à tout le moins contenir les renseignements suivants : (a) un résumé des interventions réalisées au cours de la semaine, ainsi que les prochaines étapes de la mise à l'essai; (b) une copie du rapport de suivi des défauts le plus récent. L'entrepreneur doit transmettre le rapport au chargé de projet au début de chaque semaine de mise à l'essai.
	TM.05	Une fois achevés les essais portant sur l'utilisateur final, l'entrepreneur doit transmettre au chargé de projet le rapport de clôture des essais. Celui-ci comprend la copie finale du rapport de suivi des défauts, ainsi que les jeux d'essai approuvés par les employés chargés des essais et l'ensemble des autres documents et données pertinents. Le rapport doit être accepté et approuvé par le chargé de projet.
	TM.06	Une fois les essais achevés et avant l'étape de la production, l'entrepreneur doit remettre au chargé de projet le dossier des spécifications fonctionnelles, dans lequel se trouvent consignées toutes les spécifications fonctionnelles créées et mises à l'essai dans le cadre de la solution.
	TM.06.A	Fournir la matrice de traçabilité complète des exigences dûment remplie.
	TM.07	L'entrepreneur doit fournir une série de scripts d'essais de régression dont pourra se servir le SSI pour faciliter la mise à l'essai des fonctionnalités de base des versions futures de la solution.
	TM.08	L'entrepreneur doit fournir une présentation de possibilités à l'approbation du chargé du projet en ce qui concerne les défauts rencontrés qui on un impact significatif sur la conception de la solution, le calendrier etc. ou selon les exigences du chargé du projet.
Gestion des essais (type d'essais)	TM.09	L'entrepreneur doit : (a) effectuer, sur chacun des modules ou composant de la solution, des essais unitaires, des analyses de dépendance, ainsi que des essais fonctionnels et d'intégration; (b) créer et fournir des scripts d'essai; (c) consigner et corriger tous les défauts relevés avant de passer à l'étape d'essai suivante; (d) veiller à ce que les cycles d'essai se poursuivent jusqu'à l'achèvement d'un cycle complet exempt de nouveau bogue ou défaut.

Catégorie	Section de l'EDT	Exigence
		L'achèvement de la mise à l'essai doit recevoir l'approbation finale du chargé de projet.
	TM.10	L'entrepreneur doit : (a) une fois les essais fonctionnels terminés (notamment les essais de régression, de bout en bout et les scénarios), coordonner les essais d'acceptation par les utilisateurs; (b) élaborer et fournir des scripts d'essai (y compris les essais de régression); (c) veiller à ce que les employés chargés des essais soient en mesure de consigner les défauts, bogues et anomalies, que ceux-ci se rattachent ou non à un jeu d'essai ayant été documenté; (d) veiller à ce que les cycles d'essai se poursuivent jusqu'à l'achèvement d'un cycle complet exempt de nouveau bogue ou défaut. (e) L'entrepreneur a la responsabilité de consigner tous les essais et de résoudre toutes les questions qui s'y rattachent avant de demander l'autorisation finale du chargé de projet.
	TM.11	L'entrepreneur doit mener des essais de validation des données et s'assurer de l'exactitude des données qui passeront des systèmes en place à la nouvelle solution. L'achèvement des essais de validation des données doit recevoir l'approbation finale du chargé de projet.
	TM.12	L'entrepreneur doit effectuer des essais de rendement et des essais de charge liés à la solution.

PARTIE 7 : GESTION ET SURVEILLANCE

La présente partie décrit les exigences relatives au projet et à la gestion du changement organisationnel en ce qui a trait à la solution.

1.1 GOUVERNANCE DU PROJET

L'entrepreneur est responsable de la conception, du développement et de la mise en œuvre de la solution, ce qui comprend les services de transformation des activités. L'entrepreneur assure les services suivants, sans pour autant s'y limiter :

(a) gestion et planification de projet;
(b) gestion du changement, y compris la formation et les communications;
(c) réingénierie des processus opérationnels;
(d) architecture et conception de la solution;
(e) développement et mise en œuvre de la solution;
(f) migration des données.

Globalement, TPSGC assume les responsabilités suivantes :

(a) parrainer l'ensemble du projet et en encadrer la gestion;
(b) examiner les produits livrables, fournir une rétroaction et donner son approbation en temps opportun;
(c) fournir des renseignements et des conseils à l'entrepreneur quant aux exigences fonctionnelles et non fonctionnelles;
(d) coordonner, au nom de l'entrepreneur, l'accès à des experts en la matière en ce qui a trait aux exigences fonctionnelles et non fonctionnelles;
(e) coordonner, au nom de l'entrepreneur, les rencontres qu'exige l'approbation des produits livrables (p. ex. l'architecture d'entreprise liée à la solution) lorsqu'il faut faire appel à des intervenants extérieurs au projet de transformation des systèmes de sécurité industrielle (TSSI);
(f) obtenir l'approbation du GC pour chaque point de contrôle;
(g) assurer la gestion des contrats.

La structure du projet de TSSI englobe plusieurs sous-structures, chacune remplissant une fonction particulière.

(a) **TPSGC – Secteur de la sécurité industrielle (chargé de projet)**
Le Secteur de la sécurité industrielle (SSI) est le chargé de projet et agit au nom du secteur d'activité. Le SSI assume la responsabilité globale du projet et se charge des approbations. Les fonctions suivantes lui incombent, mais de façon non limitative :
   i. prendre les décisions qui ont des répercussions sur les activités ou sur le projet;
   ii. examiner et approuver toutes les activités et l'ensemble des produits livrables du projet – formation, communications, mise en correspondance des processus opérationnels, stratégies, plans, etc.;
   iii. assurer la recherche et la coordination de l'expertise opérationnelle nécessaire au soutien des activités liées au projet – responsables des essais, analystes des activités et autres;
   iv. soutenir l'entrepreneur en ce qui a trait aux travaux que requiert la réingénierie des processus opérationnels, à la migration des données, à la gestion du changement, ainsi qu'à l'élaboration

de stratégies et de plans qui donneront lieu à la nécessaire transition de l'organisation de son état actuel à son état futur.

(b) **TPSGC – Direction générale du dirigeant principal de l'information (DGDPI)**
La Direction générale du dirigeant principal de l'information (DGDPI) de TPSGC représente le volet technique du projet, que ce soit du point de vue de TPSGC ou de celui de Services partagés Canada (SPC). La DGDPI a la responsabilité d'assurer à l'équipe de projet des services de coordination de la TI et de soutien technique. Les fonctions suivantes lui incombent, mais de façon non limitative :

i. représenter les intérêts de la DGDPI de TPSGC dans le cadre du projet de TSSI dans les domaines touchant l'architecture de la solution, la sécurité du système, la conformité aux normes relatives au Web, la maintenabilité de la solution, etc.;
ii. examiner et approuver les produits livrables de nature technique (TI) – architectures, spécifications liées à la conception, etc.;
iii. veiller à ce que les diverses entités de la DGDPI de TPSGC qui prennent part à la solution de TSSI (architecture d'entreprise de la TI, infrastructure de TI, sécurité de la TI, soutien des applications et des bases de données, etc.) participent au projet autant qu'il le faut.

(c) **Services partagés Canada**
La solution est mise en œuvre par l'entrepreneur à l'aide de l'infrastructure que lui fournit Services partagés Canada (SPC) : serveurs, réseaux, bases de données, etc. SPC travaille en collaboration avec l'entrepreneur et assume les responsabilités suivantes, sans pour autant s'y limiter :

i. concevoir et mettre en œuvre l'infrastructure qui soutient la solution et en permet la réalisation;
ii. passer en revue les mécanismes de sécurité et s'assurer qu'ils protègent également l'infrastructure;
iii. prendre part s'il y a lieu aux essais de rendement et aux essais de charge, ainsi qu'à l'établissement de la taille de l'infrastructure;
iv. participer à l'évaluation et au processus d'autorisation des mécanismes de sécurité en ce qui touche l'infrastructure.

1.2 APERÇU DES EXIGENCES – GESTION DE PROJET

L'entrepreneur doit mettre en œuvre la solution selon les indications fournies dans l'énoncé des travaux, en collaboration avec TPSGC. Le Ministère facilitera et coordonnera l'accès à l'environnement de travail. Il incombe à l'entrepreneur de fournir tous les services de gestion de projet et de contrôler la qualité des travaux effectués par son personnel des services professionnels. L'entrepreneur doit assurer tous les services de gestion de projet nécessaires pour planifier, gérer et accomplir tous les travaux visés par le contrat. Ces services sont décrits ci-dessous. Il doit offrir ces services dès l'attribution du contrat, sous réserve de l'examen et de l'approbation du chargé de projet.

1.3 EXIGENCES DÉTAILLÉES – GESTION DE PROJET

L'entrepreneur doit répondre, sans pour autant s'y limiter, aux exigences relatives à la gestion du projet énumérées dans le tableau ci-dessous.

Catégorie	Section de l'EDT	Exigence
Généralités	PM.01	L'entrepreneur doit veiller à ce que tous les travaux à accomplir soient pleinement intégrés aux activités de TPSGC de telle sorte que la portée, le rendement, le temps, la

Catégorie	Section de l'EDT	Exigence
		qualité et les éléments problématiques et de risque liés au contrat soient parfaitement gérés, contrôlés et organisés.
	PM.02	Conformément aux pratiques exemplaires de l'industrie et à la politique relative au Système national de gestion de projet, l'entrepreneur doit utiliser une méthode de gestion de projet officielle afin de garantir que les travaux qui seront accomplis pendant toute la durée du contrat satisferont aux exigences de l'EDT, de ses pièces jointes et des documents de référence.
	PM.03	L'entrepreneur doit transmettre tous les documents en version électronique au chargé de projet, dans les formats suivants : (a) documents texte ou présentations réalisés au moyen d'une application Microsoft Office (Word, PowerPoint, Excel ou Access), version 2013 ou une version ultérieure; (b) diagrammes et organigrammes – Microsoft Visio 2013 ou une version ultérieure; (c) plans de projet et calendriers – Microsoft Project 2013 ou une version ultérieure. L'entrepreneur peut demander au chargé de projet de l'autoriser à fournir des documents dans d'autres formats électroniques; ce dernier doit expressément l'autoriser. Cette approbation est accordée à la discrétion exclusive du Canada.
Équipe de gestion de projet	PM.04	L'entrepreneur doit former une équipe de gestion de projet. Il choisit à sa discrétion les membres de cette équipe, mais celle-ci doit satisfaire aux exigences minimales présentées ci-dessous. (a) L'équipe doit être dirigée par un gestionnaire principal de la prestation de services ou un gestionnaire de projet qui est responsable de la gestion et de la supervision de l'intégration et de la configuration de la solution décrites dans le présent contrat. Ce dernier doit se consacrer à temps plein au projet de TSSI. Il doit travailler sur place à TPSGC, dans la région de la capitale nationale (RCN). Le gestionnaire agit à titre de ressource de l'entrepreneur en ce qui concerne la communication de l'état du projet, des risques, des problèmes, des écarts et des mesures correctives, et agit à titre d'intermédiaire entre TPSGC et l'entrepreneur. (b) Il prépare et tient à jour un document décrivant le modèle organisationnel de l'entrepreneur. Le nom de chacun des membres de l'équipe de gestion du projet et leurs liens hiérarchiques doivent figurer dans le modèle organisationnel de l'entrepreneur. (c) Le gestionnaire prépare et tient à jour un document faisant état du modèle de gouvernance utilisé, et comportant une matrice des rôles et responsabilités, y compris les entités de l'entrepreneur et celles du GC prenant part au projet. (d) L'équipe de gestion de projet de l'entrepreneur doit se trouver sur les lieux durant toute la durée du contrat en vue de faciliter les activités de planification, de conception, de développement, de mise à l'essai et de déploiement. (e) Tous les travaux liés au projet dans le cadre desquels l'entrepreneur doit avoir un accès direct aux renseignements et aux biens des systèmes de sécurité intégrés (SSI) doivent être effectués sur place, pour la durée des travaux. À la

Catégorie	Section de l'EDT	Exigence
		suite de l'achèvement des travaux requis, il n'est plus nécessaire que ces ressources soient sur place. (f) Sauf indication contraire, tous les travaux liés au projet n'exigeant pas un accès direct aux renseignements et aux biens du SSI peuvent être réalisés ailleurs.
Services professionnels – Ressources	PM.05	Pendant toute la durée du contrat, l'entrepreneur doit fournir des employés des services professionnels qualifiés pouvant produire, réaliser et mettre en œuvre les produits livrables décrits dans l'annexe A.
Plan de projet	PM.05.A	L'entrepreneur doit élaborer un plan de gestion de projet préliminaire qui tient compte de la stratégie du soumissionnaire pour assurer la mise en œuvre réussie des exigences décrites aux sections 2 à 7 de l'ANNEXE A. Le plan doit s'harmoniser avec le cadre du Système national de gestion de projet (SNGP).
	PM.06	Élaborer et tenir à jour un plan de gestion de projet qui respecte les pratiques exemplaires ou les normes de l'industrie et qui doit être approuvé par le chargé de projet. Le Canada évaluera le plan de gestion de projet proposé par le soumissionnaire selon le degré auquel il satisfait les éléments requis suivants et la façon dont il favorise l'atteinte des résultats escomptés précisés aux sections 1 et 7 de l'ANNEXE A, notamment : (a) le document sur la gouvernance du projet et la structure de l'équipe du projet; (b) le plan de gestion de la portée; (c) le plan de gestion du calendrier; (d) le calendrier de projet; (e) le plan de gestion des risques; (f) le plan de gestion de la qualité.
Calendrier de projet	PM.07	L'entrepreneur doit : (a) en collaboration avec le chargé de projet et conformément à l'annexe A, créer, tenir à jour et surveiller le calendrier de projet détaillé, y compris les liens de dépendance et la personne responsable du suivi (BPR); (b) mettre en œuvre, tenir à jour et utiliser le calendrier de projet approuvé pendant toute la durée du contrat; tout changement qui pourrait avoir des répercussions sur le calendrier de projet ne peut être apporté que sur l'obtention d'une demande de changement approuvée; (c) les changements apportés au calendrier de projet à la suite d'une demande de changement doivent être intégrés au registre des risques du projet. (d) garder une mise à jour du calendrier de projet pendant la progression du projet ou a la demande du chargé de projet.
Surveillance du projet	PM.08	En collaboration avec le chargé de projet, l'entrepreneur doit créer et conserver le Registre des mesures de suivi – lequel fournit la liste de toutes les mesures à prendre en précisant si elles sont en attente ou si elles ont été mises en place – et doit le mettre à jour au moins une fois par semaine ou au besoin. L'entrepreneur n'a pas à fournir ce produit livrable dans le format exact présenté ci-dessous, mais le document doit comporter tous les renseignements suivants : (a) le numéro de la mesure à prendre;

Catégorie	Section de l'EDT	Exigence
		(b) la description de la mesure à prendre; (c) le nom de la personne responsable du suivi (BPR); (d) la date de mise en œuvre; (e) la date d'échéance; (f) l'état; (g) le pourcentage d'achèvement par rapport au calendrier de référence; (h) des commentaires.
	PM.09	En collaboration avec le chargé de projet, l'entrepreneur doit créer et tenir à jour l'ordre du jour des réunions de projet, au besoin. L'ordre du jour doit être communiqué aux participants au moins un jour avant la réunion. L'entrepreneur n'a pas à fournir ce produit livrable dans le format exact présenté ci-dessous, mais le document doit comporter tous les renseignements suivants : (a) l'objet; (b) la date de la réunion; (c) l'heure de la réunion; (d) le lieu de la réunion; (e) les participants convoqués; (f) les participants dont la présence est facultative; (g) la liste des mesures de suivi à examiner ou à débattre; (h) les pièces jointes, le cas échéant.
	PM.10	En collaboration avec le chargé de projet, l'entrepreneur doit créer et tenir à jour le compte rendu des réunions de projet, au besoin. Le compte rendu doit être communiqué aux participants dans les deux jours suivant la réunion. L'entrepreneur n'a pas à fournir ce produit livrable dans le format exact présenté ci-dessous, mais le document doit comporter tous les renseignements suivants : (a) le titre de la réunion; (b) la date et l'heure de la réunion; (c) les présences et les absences; (d) le nom de la personne ayant rédigé le compte rendu; (e) le nom des destinataires du compte rendu; (f) le compte rendu des discussions; (g) le compte rendu des décisions; (h) les mesures de suivi proposées; (i) les autres questions; (j) les renseignements sur la prochaine réunion.
	PM.11	En collaboration avec le chargé de projet, l'entrepreneur doit créer et tenir à jour les rapports sur l'état du projet. Ces rapports doivent être présentés et remis chaque semaine ou sur demande et comprendre à tout le moins les renseignements suivants : (a) l'état d'avancement des jalons; (b) l'information sur la situation et les problèmes liés aux dates d'achèvement; (c) la détermination de tout nouveau risque visant les produits livrables et un aperçu des stratégies d'atténuation des risques déjà déterminés; (d) toute demande de changement.

Catégorie	Section de l'EDT	Exigence
	PM.12	L'entrepreneur doit présenter au GC des procédures de gestion des demandes de changement. Celles-ci doivent comprendre à tout le moins : (a) les rôles et les responsabilités des ressources de l'entrepreneur en matière de gestion des demandes de changement; (b) la façon dont l'entrepreneur utilisera le processus de gestion des demandes de changement pour soutenir le développement de la solution; (c) la méthode employée pour distinguer les éléments de configuration; (d) la méthode d'identification des éléments de configuration; (e) la description du processus de gestion des demandes de changement, y compris le processus d'examen et d'approbation du changement; (f) les modes d'identification des éléments de configuration à employer tout au long du cycle de développement des systèmes ainsi que le processus de gestion de la configuration de ces éléments; (g) les mesures utilisées pour appliquer uniquement les changements autorisés; (h) les procédures qu'utilisera l'entrepreneur pour accepter les éléments de configuration modifiés ou nouvellement créés; (i) un registre de la gestion des demandes de changement.
	PM.13	L'entrepreneur doit s'assurer que les principaux membres de l'équipe de projet assistent à tous les événements relatifs aux étapes du projet et aux examens du projet, y compris à toute autre réunion prévue entre le chargé de projet et l'entrepreneur a la demande du chargé de projet.
	PM.14	En collaboration avec le chargé de projet, l'entrepreneur doit créer et tenir à jour le registre des risques et le journal des problèmes tout au long du cycle de vie du projet. Ces rapports doivent à tout le moins inclure : (a) des numéros d'identification; (b) des descriptions; (c) des stratégies d'intervention ou d'atténuation; (d) les probabilités de concrétisation du risque et les conséquences possibles.
Plan de projet	PM.15	En collaboration avec le chargé de projet, l'entrepreneur doit créer et tenir à jour un journal des problèmes du projet au long du cycle de vie du projet. L'entrepreneur doit transmettre une mise à jour du journal au chargé de projet si ce dernier lui en fait la demande. Ces rapports doivent à tout le moins inclure : (a) Numéro d'identité; (b) Description; (c) Réponse/gestion d'atténuation des risques; et (d) Impact et probabilité des risques.
Mise en œuvre du projet	PM.16	L'entrepreneur doit fournir un plan de livraison pour la solution qui adresse les activités et les résultats attendus en adhérant au calendrier du projet, la mise en œuvre progressive, les cycles récurrents de communication, le plan d'essaie et les cycles de formations. Les produits livrables identifiés dans le plan de livraison de solutions devraient être reflétés dans les activités de planification du projet et dans le plan de

Catégorie	Section de l'EDT	Exigence
		gestion du changement. Le plan de mise en œuvre de la solution doit également être aligné sur les étapes du projet décrites dans l'appendice 2 à l'annexe A.
Fermeture du projet	PM.17	L'entrepreneur doit préparer et fournir un rapport de clôture de projet qui inclut, sans toutefois s'y limiter : (a) Évaluation de la performance du projet; (b) Identification des enseignements tirés; (c) La confirmation que les activités contractuelles essentielles et les autres activités de fermeture de projets ont été achevées; (d) Questions en suspens; (e) Transfer of assets, deliverables and ongoing administrative functions; and (f) Mesure des avantages / résultats mise en œuvres (IRC) fournis par le projet.

2.1 APERÇU DES EXIGENCES – GESTION DU CHANGEMENT

L'intégration d'un nouveau système de soutien à la prestation des services du Secteur de la sécurité industrielle (SSI) représentera un changement considérable en ce qui a trait aux activités et aux processus que les intervenants utilisant le système actuel connaissent déjà. Ces intervenants sont notamment le personnel de l'industrie, des autres ministères, de TPSGC et du Secteur de la sécurité industrielle (SSI). Le changement devra être géré à la manière d'un processus au niveau individuel et organisationnel.

Le SSI exigera l'élaboration et la mise en œuvre d'une stratégie de gestion du changement pour assurer l'adoption précoce, itérative et réussie du nouveau système. Ces services comprendront l'identification des parties concernées, l'élaboration et la mise en œuvre d'une stratégie de participation adaptée à chacune de ces parties, ainsi que les communications et la formation afférentes, y compris tous les produits livrables, les produits documentaires, les outils et les documents connexes.

Le but de la gestion du changement consiste à assurer une transition progressive et en douceur, et l'adoption ultime du nouveau système par tous les publics et tous les intervenants.

En vue d'aider les particuliers et les organisations à bien gérer le changement, il faut se pencher sur les questions suivantes :

(a) sensibilisation (Awareness) à la nécessité du changement;
(b) désir de participer au changement et de le soutenir;
(c) connaissance des façons de changer;
(d) capacité de mettre en œuvre les compétences et les comportements nécessaires;
(e) obstacles à la réalisation fructueuse du changement;
(f) renforcement en vue de soutenir le changement;
(g) état de préparation.

Une gestion du changement efficace vise à :

(a) éviter l'interruption du service assuré aux Canadiens;
(b) faciliter l'adoption du processus et la transition terminologique pour tous les utilisateurs des systèmes, y compris les utilisateurs externes et internes;
(c) garantir l'utilisation appropriée, conforme et rapide du nouveau système ainsi que l'entrée de données dans le nouveau système;
(d) veiller à la qualité et à l'intégrité des services fournis.

La gestion du changement sera planifiée, gérée et surveillée au moyen :

(a) de plans de formation explicites et élaborés à l'avance à l'intention de tous les intervenants concernés par le système (centre d'expertise du SSI, formateurs du SSI, préposés au traitement, industrie, autres ministères, TI de DGDPI, etc.);
(b) d'un plan de communication explicite, élaboré à l'avance et modulé en fonction de la fréquence et du contenu des communications à l'intention de tous les intervenants;
(c) de documents de formation, de trousses de formation en libre-service et de documents de référence;
(d) de l'inclusion et de la mobilisation rapide, soutenue et constante aux utilisateurs de la Solution, afin qu'il apprenne graduellement, se familiarise avec le système, l'adopte et l'utilise efficacement avant son lancement;
(e) de l'évaluation précoce des risques possibles associés à la gestion du changement, des répercussions de ces risques et des mesures d'atténuation à consigner au registre des risques liés au projet.
(f) de la production d'un rapport sur la gestion du changement qui suivra constamment les activités en cours et à venir, les approches adoptées en matière de gestion du changement, et qui évaluera les activités achevées.

2.2 EXIGENCES DÉTAILLÉES – GESTION DU CHANGEMENT

2.1.1 Approche de gestion du changement

L'entrepreneur doit répondre, sans pour autant s'y limiter, aux exigences relatives à la gestion du changement énumérées dans le tableau ci-dessous.

Catégorie	Section de l'EDT	Exigence
Approche en matière de gestion du changement	CM.01	L'entrepreneur doit fournir au chargé de projet une ébauche de stratégie de gestion du changement aux fins d'examen et d'approbation. La stratégie de gestion du changement doit à tout le moins comprendre une stratégie générale fondée sur une évaluation du projet, des risques et des intervenants, qui inclut les éléments décrits ci-dessous. (a) Une évaluation permettant de comprendre les aspects suivants : i. le changement (contexte et répercussions du changement, souplesse à l'égard du changement [état de préparation]); ii. le projet; iii. l'évaluation des risques liés au changement; iv. l'identification et la mise en correspondance des intervenants; v. les connaissances et les compétences nécessaires de la part des intervenants; vi. les changements organisationnels qui mettent en évidence les principaux secteurs visés par le changement et ses répercussions

Catégorie	Section de l'EDT	Exigence
		possibles. (b) Une stratégie de communication axée sur les secteurs visés par le changement et sur les intervenants touchés. (c) Une stratégie de formation axée sur les secteurs visés par le changement et sur les intervenants touchés. (d) Une analyse des lacunes pour déterminer les besoins en ce qui a trait à la participation, aux communications et à la formation. (e) La « stratégie de gestion du changement la mieux adaptée », qui permet de cerner le concept général pertinent pour la réalisation du changement en fonction de l'évaluation. Cette stratégie doit porter sur les avantages de l'approche, la façon de faire participer les intervenants, la durabilité et l'évaluation de l'état de préparation opérationnelle. (f) Une discussion sur l'approche de transition s'appuyant sur les pratiques exemplaires. (g) Les critères de réussite de la transition et les modalités d'évaluation de cette réussite. (h) La détermination des leviers de changement dont dispose l'équipe de projet. (i) Les attentes relatives à l'affectation des ressources liées au changement suivant les étapes et les jalons du projet. (j) Des évaluations de l'état de préparation du processus et des intervenants pour chaque mise en service.

2.2.2 Plan de gestion du changement

L'entrepreneur doit fournir and maintenir le plan de gestion du changement une fois que la stratégie du changement a été approuvée par le chargé de projet. L'ébauche du plan de gestion du changement est sujet à l'approbation et la revue finale du chargé de projet. Ce plan doit comprendre les éléments suivants :

(a) Un plan relatif à l'état de préparation opérationnelle; et
(b) Un plan de communication ; et
(c) Un plan de formation;

Catégorie	Section de l'EDT	Exigence
	CM.01.A	Préparer un plan de gestion du changement préliminaire qui comprend, sans s'y limiter, les éléments suivants : A. Compréhension approfondie des exigences en matière de gestion des changements; B. Prendre en considération les points ci-après : i. Éviter l'interruption du service aux Canadiens; ii. Faciliter l'adoption du processus et les transitions terminologiques pour tous les utilisateurs, incluant les utilisateurs externes et le personnel interne;

Catégorie	Section de l'EDT	Exigence
		iii. Garantir l'utilisation appropriée, conformer et rapide du nouveau système ainsi que l'entrée de données dans le nouveau système; iv. Veiller à la qualité et à l'intégrité des services fournis. C. Méthode d'évaluation exhaustive pour évaluer l'efficacité des activités de gestion des changements.
Généralités	CM.02	Préparer un plan de gestion des changements après que le Canada a évalué le plan de gestion des changements préliminaire et déterminé qu'il appuie la transition réussie d'un état de départ vers un état ciblé et démontre les exigences énoncées ci-dessus. Le plan de gestion des changements doit être intégré au plan de gestion de projet et au calendrier de projet.
	CM.03	L'entrepreneur doit : (a) élaborer des processus et des procédures visant à institutionnaliser le changement; (b) recenser les activités relatives à la gestion du changement et les relier aux divers jalons; (c) harmoniser ses travaux avec les calendriers de formation, les communications et les approches; (d) harmoniser ses travaux avec les calendriers des activités de transition liées à la restructuration des processus; (e) cerner les attentes relatives à l'affectation des ressources liées au changement suivant les étapes et les jalons du projet; (f) déterminer la nature des ressources du GC que nécessitera la gestion du changement, le moment où on fera appel à ces ressources et la période pendant laquelle on les utilisera; (g) déterminer les secteurs présentant des risques élevés ainsi que les répercussions possibles de la matérialisation de ces risques sur la réussite du changement, élaborer des stratégies d'atténuation, recommander des mesures d'atténuation et transmettre les résultats au GC; (h) trouver des moyens rapides et efficaces de simplifier les activités de gestion du changement; (i) collaborer avec le GC pour exécuter la stratégie et le plan de gestion du changement; (j) mettre en œuvre les activités d'assainissement relatives à la gestion du changement qui seront nécessaires au long du cycle de vie du projet; (k) formuler des recommandations sur la ligne de conduite optimale à adopter pour traiter et résoudre les problèmes propres aux intervenants; (l) appuyer les ressources reconnues pour se faire les championnes du changement; (m) coordination entre les différentes composantes de la gestion du changement et les autres activités du projet. (n) Fournir un plan de soutien en service qui prévoit le transfert des

Catégorie	Section de l'EDT	Exigence
		connaissances relatives aux activités;
Plan de préparation opérationnelle	CM.04	L'entrepreneur doit fournir au chargé de projet une ébauche de plan de préparation opérationnelle aux fins d'examen et d'approbation. Ce plan comprendra : (a) une évaluation des activités en cours; (b) les critères de détermination de l'état de préparation au changement; (c) l'évaluation de l'état de préparation au début du développement; (d) une réévaluation de l'évolution de la gestion du changement et de l'état de préparation opérationnelle à mesure qu'avance le projet et avant chaque mise en service; (e) une évaluation des mesures correctives reposant sur les évaluations de l'état de préparation et un compte rendu de la situation à l'intention du GC.
Plan de communication	CM.05	L'entrepreneur doit fournir au chargé de projet une ébauche de plan de communication aux fins d'examen et d'approbation. (a) Ce plan de communication général doit porter sur les aspects suivants : i) les avantages du projet de TSSI; ii) la façon dont les activités de préparation opérationnelle du GC seront accomplies; iii) la façon dont les utilisateurs peuvent soutenir l'effort de transition du GC; iv) les travaux relatifs à la transition; v) l'évaluation postérieure à la migration pour améliorer les activités de transition à venir; vi) un calendrier, des messages clés et des médias pour chaque étape du projet. (b) La mobilisation des dirigeants en vue du changement : confirmer l'appui des dirigeants, créer des rôles de défenseurs du changement, offrir l'encadrement et les outils qui faciliteront ce rôle de chef de file. (c) Réseau du changement : établir un réseau de défenseurs du changement au sein du SSI et solliciter la participation des dirigeants afin qu'ils apportent un soutien actif et se fassent les chefs de file du changement. (d) Recenser les activités de communication tout au long du cycle de vie du projet et signaler les obstacles potentiels à la mise en œuvre de ces activités, ainsi que les solutions possibles. (e) Adopter une approche de rétroaction et un plan de mesures correctives pour les secteurs de la gestion du changement qui requièrent des améliorations.
		L'entrepreneur doit :

Catégorie	Section de l'EDT	Exigence
Prestation des communications	CM.06	(a) procéder à l'évaluation et à la mise à jour des activités de communication en fonction des risques et des enjeux du projet, et fournir une évaluation de l'aide que peuvent apporter ces activités quant aux mesures d'atténuation à prendre; (b) animer des ateliers en vue de discuter des changements, de les analyser et de les valider; (c) présenter des séances d'information selon diverses formules – validation de principe, exercices pratiques permettant de faire l'essai du système, remue-méninges et autres; (d) consigner les commentaires relatifs aux communications et produire un rapport décrivant la réussite des activités de communication réalisées; (e) élaborer et transmettre des documents se rattachant aux activités de communication et de mobilisation, y compris, mais sans s'y limiter, des présentations, un programme, des brochures d'information, des communications à l'intention des intervenants et autres; (f) réévaluer les activités de communication selon l'état de préparation organisationnelle et les conclusions des rapports, et présenter des recommandations; (g) collaborer avec le GC à l'exécution de toutes les activités de communication destinées aux intervenants internes de TPSGC, ainsi qu'aux utilisateurs des autres ministères et de l'industrie.
Plan de formation	CM.07	L'entrepreneur doit fournir au chargé de projet une ébauche de plan de formation aux fins d'examen et d'approbation. (a) Le plan de formation doit à tout le moins décrire l'approche adoptée et préciser comment l'entrepreneur entend : i) définir les compétences et le niveau de compétences nécessaires pour soutenir l'application sur le plan des connaissances opérationnelles, des connaissances liées à l'application et des connaissances relatives à la solution; ii) décrire la façon dont les utilisateurs seront évalués pour s'assurer qu'ils comprennent bien leur rôle et les capacités du système; iii) trouver des méthodes, des procédures et des documents qui permettront d'assurer la formation, de réaliser des essais d'acceptation par les utilisateurs et d'effectuer le transfert des connaissances; iv) trouver une approche en vue de recueillir les commentaires des participants à la formation sur les aspects qui nécessitent des améliorations et sur ceux qui constituent une réussite; cerner les aspects de la solution susceptibles de présenter des faiblesses ou de nécessiter une amélioration de la formation; v) procéder à l'évaluation des besoins en formation par type d'utilisateurs; cette évaluation doit comprendre les besoins initiaux, évolutifs et exhaustifs en formation sur la solution ainsi que les besoins continus en formation des nouveaux utilisateurs

Catégorie	Section de l'EDT	Exigence
		et en formation d'appoint. (b) Le plan de formation des utilisateurs doit à tout le moins comprendre les éléments suivants : i) les étapes de formation prévues entre le début de 2018 et mars 2019; ii) une description claire des besoins en formation; iii) une description claire des méthodes et des documents d'enseignement propres à chaque type d'utilisateurs; iv) une description de la façon dont les utilisateurs seront évalués pour faire en sorte qu'ils comprennent bien leur rôle et les capacités du système; v) une définition des compétences et du niveau de compétences nécessaires pour soutenir l'application sur le plan des connaissances opérationnelles, des connaissances liées à l'application et des connaissances relatives à la solution; vi) des liens entre les activités de formation prévues et le plan de communication relatif à la gestion du changement; vii) la synchronisation du calendrier des activités de formation et des activités de restructuration des processus; viii) des instructions sur la manière de trouver des ressources en matière de formation; ix) des précisions sur les résultats attendus de la part des utilisateurs; x) des instructions détaillées concernant chaque approche de transition, notamment ce qui suit : (1) les outils et les ressources qui seront offerts; (2) la manière de remplir les profils d'utilisateur; (3) une foire aux questions; (4) des instructions sur la communication de la rétroaction pendant la transition. (c) Le plan de formation des agents du bureau de service de niveau 2 doit au moins comprendre les éléments suivants : i) le calendrier des activités de transition; ii) la description des droits d'accès, des rôles et des responsabilités des agents du bureau de service de niveau 1 pendant la migration du GC; iii) des instructions sur la manière de trouver des ressources en matière de formation; iv) les procédures d'acheminement aux paliers hiérarchiques supérieurs. (d) Le plan de formation des administrateurs autorisés doit au moins comprendre les éléments suivants : i) le calendrier des activités de transition; ii) la description des droits d'accès, des rôles et des responsabilités du GC et de ses administrateurs pendant la migration du GC; iii) des instructions sur la manière de trouver des ressources en matière de formation.

Catégorie	Section de l'EDT	Exigence
Prestation de la formation	CM.08	L'entrepreneur doit réaliser les activités énumérées ci-dessous, qui comprennent une formation technique complète et une formation des utilisateurs, des communications efficaces, ainsi que la participation fructueuse des intervenants. (a) Fournir les procédures d'utilisation normalisées de bout en bout et axées sur les processus qui décrivent les principales activités et responsabilités de l'utilisateur, en vue d'informer les utilisateurs des changements qui surviendront dans leurs activités quotidiennes. (b) Fournir les documents de formation permettant de s'assurer que : i) les notions pertinentes pour utiliser la nouvelle solution (préposés au traitement du SSI et utilisateurs de l'industrie) sont expliquées; ii) les notions pertinentes pour soutenir et tenir à jour la nouvelle solution (administrateurs de système du SSI, de la DGDPI et de SPC) sont expliquées. (c) Consigner les commentaires des participants à la formation et produire un rapport décrivant la réussite de la formation donnée. (d) Fournir et mettre à jour les documents de formation au besoin ou au moment de la mise en œuvre d'une version importante, afin de tenir compte des nouvelles caractéristiques et des changements apportés. Les documents de formation doivent être conformes au plan de formation approuvé. (e) Assurer une formation aux administrateurs autorisés, y compris au personnel technique sélectionné par le GC, spécifiquement en vue d'apprendre à ces participants à utiliser les fonctions et les caractéristiques de l'environnement informatique du GC. Ce type de formation peut prendre la forme d'un enseignement en classe, d'un enseignement assisté par ordinateur, d'un enseignement individuel ou d'un autre type d'enseignement. (f) Assurer une formation aux utilisateurs externes, y compris une formation précise – virtuelle ou assistée par ordinateur – (et choisie au cas par cas) et fournir des documents de référence aux utilisateurs ayant accès à la solution. (g) Assurer une formation aux utilisateurs internes à la demande du GC, y compris une formation bien précise – en classe ou assistée par ordinateur – (et choisie au cas par cas), ce qui comprend la formation à l'intention des nouveaux employés, les cours de perfectionnement et l'apprentissage de compétences spécialisées. (h) Assurer aux utilisateurs une formation des formateurs, conformément aux directives du GC. (i) Assurer aux membres du personnel du projet une formation axée sur leur rôle afin de faciliter l'exploitation complète de toutes les fonctions pertinentes avant chaque nouvelle version du produit. (j) À la demande du GC, renseigner les utilisateurs au sujet de la solution de bout en bout qui leur permettra de répondre à leurs exigences opérationnelles, et leur assurer une formation sur cette solution. (k) Fournir les documents de formation à utiliser pour le système de

Catégorie	Section de l'EDT	Exigence
		gestion de l'apprentissage SABA. (l) Démontrer la réussite de la formation en invitant des utilisateurs individuels ou des groupes d'utilisateurs à exécuter intégralement un processus préétabli. (m) Élaborer, documenter et offrir un programme de formation pour enseigner au personnel du GC tous les aspects des processus et des fonctionnalités de la solution. (n) Élaborer, documenter et fournir le contenu des modules de formation libres de droits d'auteur et de redevances pour toute modification et rediffusion par le GC. (o) Pendant la durée du contrat, l'entrepreneur doit au besoin participer à toutes les formations initiales et en cours données par le GC.
Langues officielles	CM.09	Toutes instructions, formations, communications et descriptions des rôles pour utilisateur interne et externe doit être disponible and dans la langue officielles de l'utilisateur.

PARTIE 8: MAINTIEN DE LA SOLUTION

La présente partie décrit les exigences relatives au maintien de la solution.

1.1 APERÇU DES EXIGENCES

L'entrepreneur est responsable de la conception et de l'élaboration des matériaux, des processus et des activités qui seront utilisé par le centre d'expertise du SSI et de TPSGC DDPI/SPC pour le soutien et l'entretien de la solution lors du lancement de la solution. L'entrepreneur doit s'assurer que le centre d'expertise du SSI est prêt et apte a offrir des services de formation et de soutien au utilisateur internes et externes lors de du lancement de la solution et d'assurer que TPSGC DDPI et SPC sont en mesure de fournir le soutien technique requis.

1.2 EXIGENCES DÉTAILLÉES

L'entrepreneur doit répondre, sans pour autant s'y limiter, aux exigences relatives au maintien de la solution dans le tableau ci-dessous.

Catégorie	Section de l'EDT	Exigence
Maintien de la solution	SS.01	Élaborer la totalité de la documentation relative au système, y compris en ce qui touche les aspects techniques et fonctionnels de la solution.
	SS.02	Réaliser, pour le nouveau système et les processus qui s'y rattachent, des schémas illustrant les relations entre les composants du système, ainsi qu'entre celui-ci et ses divers utilisateurs.
	SS.03	Fournir les procédures d'utilisation normalisées de bout en bout et axées sur les processus qui décrivent les principales activités et responsabilités de l'utilisateur, en vue d'informer les utilisateurs des changements qui surviendront dans leurs activités quotidiennes.
	SS.04	Élaborer, documenter et fournir une base de connaissances à laquelle le GC aura accès.
	SS.05	Préparer un guide d'administration du système.
	SS.06	Élaborer pour le système une stratégie de diffusion ininterrompue de l'information.
	SS.07	Établir un ensemble de processus qui permettront de s'assurer que le changement sera adopté et maintenu à long terme.
	SS.08	Participer à l'élaboration de processus de soutien du système.
	SS.09	Documenter et présenter des recommandations pour améliorations future.

PARTIE 9: SERVICES FACULTATIFS

Les travaux décrits dans cette section devront faire l'objet d'une demande, par le GC, par l'intermédiaire d'une autorisation de tâche, sur demande, selon l'ANNEXE E – Formulaire d'autorisation de tâches. La base de paiement contractuelle applicable à la tâche sera précisée au moment de la demande.

1.1 SERVICES SUPPLÉMENTAIRES DE RESTRUCTURATION DES PROCESSUS

En plus des services décrits à la section 2 : 1.1 et 1.2, l'entrepreneur doit fournir, sur demande, des services supplémentaires de restructuration des processus et proposer des ressources qualifiées ayant de l'expérience dans la prestation de services de restructuration des processus.

1.2 SERVICES SUPPLÉMENTAIRES DE MIGRATION DES DONNÉES

En plus des services décrits à la section 2 : 2.2.3, l'entrepreneur doit fournir, sur demande, des services supplémentaires de migration des données et proposer des ressources qualifiées ayant de l'expérience dans la prestation de services de migration des données.

1.3 DÉVELOPPEMENT ET CONFIGURATION SUPPLÉMENTAIRE DU SYSTÈME

Bien que l'énoncé des travaux définisse clairement une solution souple pouvant être configurée par le GC, le GC prévoit qu'il sera nécessaire de modifier la solution afin de tenir compte des changements apportés à l'environnement opérationnel et de la sécurité, et peut demander des services supplémentaires pour appuyer les changements apportés à la configuration du système.

En plus des services décrits à la section 2 : Exigences Opérationnelles, section 3 : Exigences Techniques, section 4 : Accès Sécurisé, section 5 : Exigences Relative a la Sécurité de la TI, sur demande, l'entrepreneur doit fournir des services supplémentaires et proposer des ressources qualifiées et ayant de l'expérience dans la prestation de services de développement et configuration supplémentaire du système.

1.4 SERVICES SUPPLÉMENTAIRES DE GESTION DES ESSAIS

In addition to the Testing Management services described in Section 6: Testing Management, the Contractor must, on an as-and-when-requested basis, provide additional Testing Management services and must propose resources that are qualified and have experience providing Testing Management services.

1.5 SERVICES SUPPLÉMENTAIRES DE GESTION DE PROJET ET DE GESTION DU CHANGEMENT

En plus des services décrits à la section 7 : Gestion et surveillance, l'entrepreneur doit fournir, sur demande, des services supplémentaires de gestion de projet et de gestion du changement et proposer des ressources qualifiées ayant de l'expérience dans la prestation de services de gestion de projet ou gestion du changement.

1.6 SERVICES SUPPLÉMENTAIRES DE MAINTIEN DE LA SOLUTION

En plus des services décrits à la section 8 : Maintien de la solution, l'entrepreneur doit fournir, sur demande, des services supplémentaires de maintien de la solution et proposer des ressources qualifiées ayant de l'expérience dans la prestation de services de maintien de la solution.

1.7 CATÉGORIES DE SERVICES PROFESSIONNELS

Pour les travaux décrits dans les sections 1.1 Services supplémentaires de restructuration des processus, 1.2 Services supplémentaires de migration des données, 1.3 Développement et configuration supplémentaire du système, 1.4 Services supplémentaires de gestion des essais, 1.5 Services supplémentaires de gestion de projet et de gestion du changement, et 1.6 Services supplémentaires de maintien de la solution, l'entrepreneur doit fournir les services professionnels indiqués à l'ANNEXE F – Renseignements sur les catégories de ressources dans le cadre des services facultatifs, sur demande, selon les taux fixes quotidiens tout compris indiqués dans l'ANNEXE B – Base de paiement, pendant toute la durée du contrat, y compris pendant toute prolongation de ce dernier lorsque l'autorité contractante exerce les options qui y sont prévues.

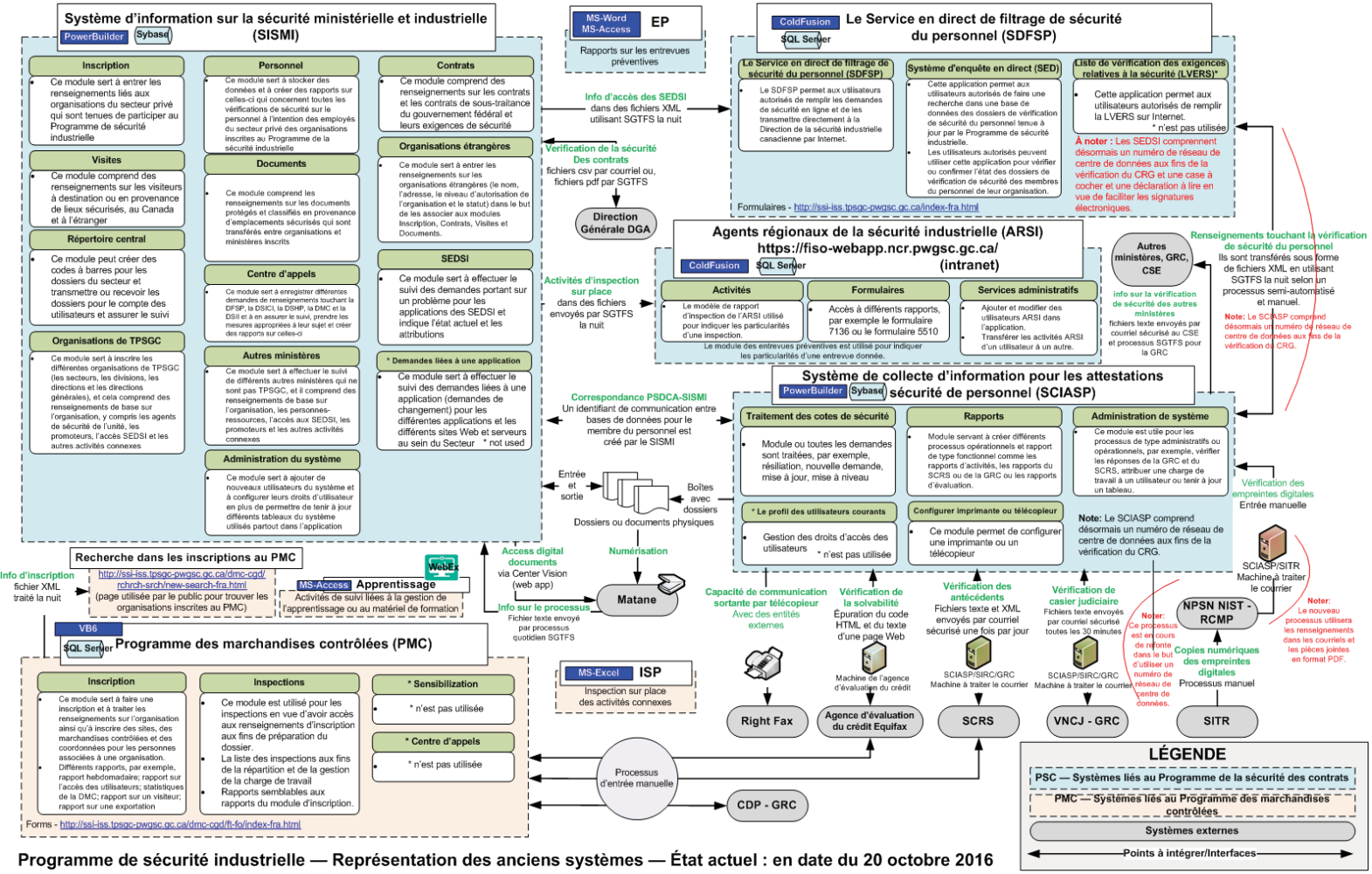
1.8 SERVICES DE SÉCURITÉ SUPPLÉMENTAIRES

En plus des services de sécurité énoncés dans la section 5, Exigences relatives à la sécurité des TI, l'entrepreneur doit fournir sur demande et selon les besoins des services de sécurité des TI supplémentaires et doit proposer des ressources qualifiées et ayant l'expérience de fournir des services de sécurité des TI.

APPENDICE 1 DE L'ANNEXE A – PROCESSUS OPÉRATIONNELS ACTUELS

APPENDICE 1 DE L'ANNEXE A – PROCESSUS OPÉRATIONNELS ACTUELS

Le présent appendice présente les processus opérationnels actuels pour l'exécution du Programme de sécurité des contrats (PSC) et du Programme des marchandises contrôlées (PMC).



Programme de sécurité industrielle — Représentation des anciens systèmes — État actuel : en date du 20 octobre 2016

1.1 PROCESSUS OPÉRATIONNELS DU PSC

1.1.1 Sécurité du contrat – Avant l'attribution du contrat

Le processus opérationnel de sécurité du contrat avant l'attribution du contrat appuie la fonction d'approvisionnement du gouvernement en assurant la sécurité des contrats attribués par Services publics et Approvisionnement Canada ou à la demande des autres ministères gouvernementaux. Les exigences relatives à la sécurité dans le cadre d'un contrat PROTÉGÉ ou CLASSIFIÉ sont notées dans la Liste de vérification des exigences relatives à la sécurité (LVERS), qui accompagne le dossier d'invitation à soumissionner; on peut étoffer ces exigences par des clauses de sécurité figurant dans le contrat lui-même. Dans le cas des contrats internationaux, le PSC communiquera avec le gouvernement étranger responsable pour recevoir une garantie de sécurité avant la divulgation des renseignements ou des biens protégés ou classifiés aux intérêts étrangers.

La LVERS fournie et les documents justificatifs des contrats sont examinés pour veiller à ce qu'ils soient complets. La révision ou la mise à jour de la LVERS peut déclencher d'autres processus du PSC. La LVERS relative au contrat de sous-traitance exige que le contrat principal soit approuvé avant que le contrat de sous-traitance puisse être mis en place pour la demande de propositions (DP). Les soumissionnaires étrangers désignés en raison du processus de DP peuvent exiger une LVERS mise à jour pour obtenir des clauses de sécurité étrangère.

Des clauses de sécurité du contrat sont fournies à l'autorité contractante selon les renseignements fournis dans la LVERS soumise. Habituellement, les clauses de sécurité sont de portée nationale, mais peuvent aussi comprendre des clauses de sécurité étrangère. Des clauses de sécurité fournies sont comprises dans les documents d'invitation à soumissionner des contrats, empêchant ainsi un accès non autorisé aux renseignements et aux biens protégés et classifiés.

Le PSC s'assure que les organisations canadiennes ont mis en place des mesures de protection appropriées pour les contrats avec les pays étrangers. À la demande des gouvernements étrangers, le PSC peut veiller à ce que les attestations de sécurité des organisations canadiennes souhaitant soumissionner des contrats étrangers de nature délicate soient confirmées. De même, le PSC peut demander auprès des gouvernements étrangers de veiller à ce que les organisations étrangères disposent de mesures de protection appropriées.

Identification du flux des travaux	**1 Flux de travaux avant l'attribution du contrat du PSC**
Unité(s) opérationnelle(s)	• Autorité contractante du client • PSC du Secteur de la sécurité industrielle (SSI) – Analyste du contrat

Objectif opérationnel	• Soumission de la LVERS par l'autorité contractante pour l'analyse et la fourniture des clauses de sécurité. • Les clauses de sécurité sont nécessaires aux fins d'intégration dans la DP du contrat.
Élément déclencheur	• Contrat avec le gouvernement du Canada (GC) qui a déterminé les exigences en matière de sécurité.
Description du flux des travaux	1. Début du processus. 2. L'autorité contractante du client précise que le contrat comporte des exigences possibles en matière de sécurité. 3. L'autorité contractante du client fournit des documents justificatifs, au besoin. 4. L'autorité contractante du client remplit et soumet une LVERS au PSC du SSI. S'il existe une LVERS et un contrat existants, l'autorité contractuelle cliente soumettrait une sous-LVERS dans le cadre d'un contrat de sous-traitance. 5. Le PSC reçoit la LVERS et procède à un triage pour déterminer si la LVERS soumise est nouvelle, une révision d'une LVERS existante ou une sous-LVERS. 6. S'il s'agit d'une nouvelle LVERS, une nouvelle entrée est créée dans l'application à l'appui existante. Passez à l'étape 17. 7. S'il s'agit d'une révision d'une LVERS existante, la LVERS existante et les renseignements relatifs au contrat sont récupérés. Passez à l'étape 17. 8. S'il s'agit d'une sous-LVERS, le PSC validera que le contrat initial existe et possède le niveau de sécurité approprié. 9. Si le contrat principal de la sous-LVERS n'existe pas, la sous-LVERS est rejetée. 10. L'autorité contractante du client qui a soumis la sous-LVERS est avisée du rejet. Passez à l'étape 16. 11. Si le contrat principal de la sous-LVERS n'existe pas, le PSC confirmera si le contrat principal a été approuvé. 12. Si le contrat principal de la sous-LVERS n'a pas été approuvé, l'autorité contractante et l'agent de sécurité d'entreprise en sont avisés. 13. Au besoin, la sous-LVERS déclenchera le processus d'inscription au PSC (3 flux des travaux pour la nouvelle inscription au PSC); autrement, passez à l'étape 16. 14. Au besoin, la sous-LVERS déclenchera le processus de mise à jour de l'inscription au PSC (flux de travaux de la mise à jour de l'inscription au PSC); autrement, passez à l'étape 16. 15. Si le contrat principal de la sous-LVERS a été approuvé, l'autorité contractante en est avisée. Selon les détails du contrat, les autres intervenants intéressés comme le Centre de la sécurité des télécommunications Canada (CSTC), le PMC du SSI, et d'autres intervenants intéressés en sont aussi avisés. Une inspection du site peut aussi être déclenchée, au besoin. La LVERS et le contrat sont marqués pour un suivi. 16. Le processus avant l'attribution du contrat prend fin. 17. Le PSC examine la LVERS soumise et tout document justificatif fourni. 18. Le PSC examine la LVERS soumise afin d'en vérifier l'exhaustivité. 19. Si la LVERS n'est pas complète, l'autorité contractante du client est avisée que la LERS doit être révisée. Le processus recommence à l'étape 4. 20. Si la LVERS est complète, le PSC indique les clauses de sécurité nationales requises selon les exigences en matière de sécurité du contrat.

	21. Si la LVERS indique qu'il existe des exigences de sécurité étrangère. La Direction de la sécurité industrielle internationale (DSII) est consultée. 22. La DSII indique les clauses de sécurité étrangère nécessaires et les fournit au PSC. 23. Le PSC renvoie toutes les clauses de sécurité indiquées à l'autorité contractante du client pour les intégrer dans la DP du contrat. 24. Si les clauses de sécurité étaient fournies pour une LVERS révisée, les intervenants intéressés comme le CSTC, le PMC du SSI, et d'autres intervenants intéressés en sont avisés. Une inspection du site peut aussi être déclenchée, au besoin. La LVERS et le contrat sont marqués pour un suivi. 25. L'autorité contractante du client ajoute les clauses de sécurité fournies dans les documents d'invitation à soumissionner des contrats. 26. Le contrat est conclu pour la DP. 27. Les soumissionnaires éventuels du contrat sont désignés. 28. S'il n'y a pas de soumissionnaire étranger éventuel, passez à l'étape 30. 29. S'il existe des soumissionnaires étrangers éventuels, le contrat et sa LVERS sont examinés pour les clauses de sécurité étrangère pour assurer la sécurité du contrat. 30. Le processus suivant l'attribution du contrat (2 flux de travaux suivant l'attribution du contrat du PSC) est déclenché.
Intrants	• LVERS
Extrants	• Clauses de sécurité nationale et étrangère • Avis aux intervenants

1.1.2 Sécurité du contrat – Après l'attribution du contrat

Le processus suivant l'attribution du contrat examine les renseignements relatifs au contrat soumis confirmant la conformité de la Politique du gouvernement sur la sécurité en déterminant si les clauses de sécurité requises étaient comprises dans le contrat, et si l'organisation retenue est inscrite au PSC et possède le niveau approprié de sécurité selon les exigences contractuelles en matière de sécurité. D'autres processus du PSC peuvent être déclenchés en raison du processus d'examen suivant l'attribution du contrat. Si toutes les exigences du contrat sont respectées, l'autorité contractante sera avisée de donner suite au contrat.

La sous-traitance est utilisée lorsqu'un détenteur de contrat principal exige que les travaux soient effectués par une autre organisation. Un sous-contrat doit être déclaré au PSC aux fins d'approbation lorsque des exigences en matière de sécurité s'imposent. La sous-traitance internationale exige que le PSC confirme l'attestation de sécurité de l'organisation étrangère avant un engagement commercial. Chaque contrat de sous-traitance exige sa propre LVERS aux fins d'approbation et obtiendra des clauses de sécurité du contrat propres au contrat de sous-traitance aux fins d'intégration dans le contrat de sous-traitance. Le niveau de sécurité d'un contrat de sous-traitance ne peut pas être supérieur à celui du contrat principal; il peut toutefois être inférieur.

Identification du flux des travaux	2 Flux de travaux suivant l'attribution du contrat du PSC
Unité(s) opérationnelle(s)	• Autorité contractante • PSC du Secteur de la sécurité industrielle (SSI) – Analyste du contrat
Objectif opérationnel	• Examen des contrats soumis confirmant la conformité de la politique sur la sécurité du gouvernement.
Élément déclencheur	• Contrat attribué avec le GC qui a déterminé les exigences en matière de sécurité.
Description du flux des travaux	1. Début du processus. 2. L'autorité contractante du client soumet les renseignements sur le contrat au PSC. Les renseignements sur le contrat peuvent être fournis directement par l'autorité contractante ou le système Environnement automatisé de l'acheteur. 3. Le PSC examine les renseignements relatifs au contrat soumis afin d'en vérifier l'exhaustivité. 4. Si les renseignements ne sont pas complets, le PSC demandera des renseignements auprès de l'autorité contractante. 5. Si les renseignements fournis sont complets, le PSC vérifie si le contrat est conforme. 6. En cas de conformité, passez à l'étape 23. En cas de non-conformité, l'un des quatre processus (étape 7, étape 9, étape 12 ou étape 15) pourrait être déclenché. En fonction de la situation, il est possible qu'un ou que plusieurs processus soient déclenchés selon des raisons de non-conformité. Si les clauses de sécurité étrangère sont manquantes ou s'il y a un problème avec l'entrepreneur étranger retenu, la DSII est consultée. 7. Si les clauses de sécurité sont absentes du contrat. 8. Le PSC communique avec l'autorité contractante du client en l'avisant des mesures requises. Passez à l'étape 30. 9. Si on indique une atteinte à la sécurité, le PSC vérifiera auprès de l'autorité contractante du client pour l'atténuer. 10. Si le PSC est satisfait de la réponse de l'autorité contractuelle du client, passez à l'étape 30. 11. Si le PSC n'est pas satisfait de la réponse de l'autorité contractante du client, une enquête est déclenchée (12 enquêtes du flux de travaux du PSC). Passez à l'étape 30. 12. Si l'entrepreneur retenu doit être inscrit au PSC. 13. L'autorité contractante du client est avisée que l'organisation contractante doit être inscrite. 14. Le processus d'inscription au PSC est déclenché (3 flux des travaux pour la nouvelle inscription au PSC). Passez à l'étape 18. 15. Si l'entrepreneur retenu est déjà inscrit, mais nécessite une mise à jour de son niveau d'autorisation de sécurité. 16. Le PSC entamera le processus de mise à jour de l'inscription de l'organisation au nom du client ou le PSC avisera le client de lancer une enquête de sécurité sur une organisation du secteur privé (ESOSP). 17. Le processus de mise à jour de l'inscription au PSC est déclenché (flux des travaux de la mise à jour de l'inscription). Passez à l'étape 18. 18. Si l'organisation contractante est considérée conforme dans le cadre du processus d'inscription, passez à l'étape 23.

	19. Si l'organisation contractante n'est pas considérée conforme dans le cadre du processus d'inscription, le PSC donnera suite au contrat. 20. Si tous les problèmes de conformité sont résolus, passez à l'étape 23. 21. Si tous les problèmes de conformité ne sont pas résolus, après un nombre prédéterminé de tentatives sans réponse, le contrat prendra fin. 22. Une enquête est déclenchée (12 enquêtes du flux de travaux). Passez à l'étape 30. 23. Les intervenants intéressés comme le CSTC, le PMC du SSI, et les autres sont avisés de l'attribution du contrat. 24. Si le contrat a des exigences en matière d'inspection comme l'inspection de la technologie d'information. S'il n'y a pas d'exigences en matière d'inspection, passez à l'étape 28. 25. L'analyste du contrat procédera à une inspection (inspection du flux des travaux). 26. Le processus d'inspection se déroule (10 Inspection du flux des travaux du PSC). 27. Si le processus d'inspection a relevé des problèmes, le contrat fait l'objet d'un suivi. 28. Si des problèmes soulevés n'ont pas été réglés, le contrat fait alors encore l'objet d'un suivi; ce cycle se poursuit jusqu'à ce que tous les problèmes relevés dans le cadre de l'inspection soient réglés. 29. Si tous les problèmes soulevés sont réglés, l'autorité contractante client est avisée d'aller de l'avant avec le contrat. 30. Fin du processus.
Intrants	• LVERS • Contrat attribué et renseignements supplémentaires • Résultats de l'enquête • Résultats de l'inspection • Nouvelle inscription ou mise à jour de l'inscription de l'organisation
Extrants	• Résiliation du contrat pour non-conformité • Avis aux intervenants • Attribution et mise en œuvre du contrat

1.1.3 Inscription au PSC – Nouvelle/mise à jour

Les services d'enquête de sécurité de l'organisation appuient l'inscription des entreprises souhaitant participer aux contrats comportant des exigences de sécurité du GC et des gouvernements étrangers. Le PSC mène une enquête de sécurité des organisations inscrites du secteur privé canadien pour veiller à ce que les organisations aient mis en œuvre des mécanismes de sécurité appropriés pour la manipulation des renseignements et des biens protégés/classifiés du GC. Les organisations doivent détenir une attestation de sécurité d'organisation avant de commencer les travaux liés au contrat comportant des exigences de sécurité du GC. Le PSC confirme ou demande des attestations auprès de partenaires étrangers pour donner l'assurance que les entreprises étrangères visées satisfont aux exigences de sécurité des contrats du GC.

Le processus opérationnel d'inscription de l'organisation comprend la réception et l'évaluation des demandes d'inscription des contrats sécurisés indiqués. Les organisations sous-traitantes exigent que l'entrepreneur principal soit déjà inscrit. Les contrats des organisations qui ne sont pas en mesure de répondre aux exigences description seront résiliés pour non-conformité.

Identification du flux des travaux	**3 Flux de travaux de la nouvelle inscription ou mise à jour de l'inscription au PSC**
Unité(s) opérationnelle(s)	• Organisme parrain • Analyste du contrat du PSC • Commis à l'inscription au PSC • Analyste de l'inscription au PSC
Objectif opérationnel	• Mener une enquête de sécurité des nouvelles organisations inscrites pour assurer la sécurité des contrats. • Mener une enquête de sécurité mise à jour des organisations inscrites pour assurer la sécurité des contrats.
Élément déclencheur	• L'organisme parrain soumet une demande pour inscrire une autre organisation ou pour mettre à jour l'attestation de sécurité existante. • L'analyste du contrat du PSC déclenche le processus d'inscription.
Description du flux des travaux	1. Début du processus. 2. L'organisme parrain ou l'analyste du contrat du PSC soumet une demande pour inscrire une nouvelle organisation ou mettre à jour une organisation existante. 3. Le commis à l'inscription au PSC vérifie si l'organisation existe déjà dans le PSC. 4. Si l'organisation existe déjà, le commis à l'inscription au PSC vérifie si le niveau de sécurité demandé est supérieur au niveau de sécurité actuel des organisations. 5. Si le niveau de sécurité demandé n'est pas supérieur au niveau de sécurité actuel des organisations. Le parrain est avisé que l'organisation parrainée est déjà inscrite. Passez à l'étape 8. 6. Si l'organisation n'existe pas déjà dans le PSC OU si le niveau de sécurité de l'organisation demandé est supérieur au niveau de sécurité existant, le type de parrain est observé. 7. Si le parrain provient de l'industrie, le commis à l'inscription au PSC vérifiera si le parrain est l'entrepreneur principal qui parraine un sous-traitant. Si non, passez à l'étape 8. 8. Le parrain reçoit une lettre de refus. 9. La demande d'inscription est close. 10. Si le commanditaire provient d'un autre ministère OU si le parrain est l'entrepreneur principal, le commis à l'inscription au PSC examine une demande d'inscription de l'organisation, lui donne un degré élevé de priorité et l'attribue à un analyste de l'inscription au PSC. 11. L'analyste de l'inscription au PSC examine la trousse d'inscription. Si la trousse d'inscription est complète, passez à l'étape 17.

	12. Si la trousse d'inscription n'est pas complète, le niveau de sécurité de l'organisation demandé est examiné et une lettre d'établissement est envoyée à l'organisation demandant des renseignements. 13. Si la documentation est fournie dans les 30 jours ouvrables, passez à l'étape 17. 14. Si la documentation exigée n'est pas fournie dans les 30 jours ouvrables, un rapport de suivi sur la lettre d'établissement est envoyé à l'organisation. 15. Si la documentation exigée est fournie dans les cinq jours ouvrables, passez à l'étape 17. 16. Si la documentation exigée n'est pas fournie par l'organisation dans les cinq jours ouvrables, la demande d'inscription est close pour non-conformité. 17. L'analyste de l'inscription au PSC examine et valide tous les renseignements fournis. 18. Si l'attestation de sécurité d'organisation concerne une vérification d'organisation désignée (VOD). 19. Le processus d'attestation de sécurité concernant une VOD est déclenché (4 flux des travaux pour l'inscription au PSC et la VOD). 20. Si l'attestation de sécurité d'organisation concerne l'attestation de sécurité d'installation (ASI). 21. Le processus d'attestation de sécurité concernant une ASI est déclenché (5 flux des travaux pour l'inscription au PSC et l'ASI). 22. Si l'attestation de sécurité d'organisation concerne l'autorisation de détenir des renseignements (ADR). 23. Le processus d'attestation de sécurité concernant une ADR est déclenché (6 flux des travaux pour l'inscription au PSC et l'ADR). 24. Le processus de nouvelle inscription/de mise à jour de l'inscription prend fin.
Intrants	• Enquête de sécurité sur une organisation du secteur privé (ESOSP) • Renseignements sur l'organisation fournis
Extrants	• Lettre d'établissement • Lettre de rejet • Avis de résiliation

1.1.4 Inscription au Programme de sécurité des contrats – Enquête de sécurité de l'organisation

Les processus opérationnels de l'enquête de sécurité pour l'inscription de l'organisation évaluent l'organisation selon le niveau de sécurité indiqué dans le contrat sécurisé et l'exigence du besoin de connaître. L'enquête de sécurité évalue la structure organisationnelle, la propriété, la situation juridique, les cadres supérieurs clés, l'agent de sécurité d'entreprise (ASE), les mesures de sécurité physique et de sécurité des technologies de l'information, etc. Les organisations qui satisfont aux exigences de sécurité des contrats portant sur les renseignements ou les biens du gouvernement canadien ou d'un gouvernement étranger obtiennent l'attestation de sécurité de l'organisation demandée, notamment la vérification d'organisation désignée (VOD), la capacité de protection des installations (CPI), l'autorisation de détenir des renseignements (ADR), etc.

Les organisations qui ne sont pas en mesure de fournir les renseignements demandés sont clôturées pour cause de non-conformité ou leur niveau d'attestation de sécurité est abaissé. En fonction du niveau d'attestation de sécurité requis pour l'organisation, d'autres processus du programme de sécurité des contrats (PSC) peuvent être déclenchés.

1.1.4.1 **Vérification d'organisation désignée**

Identification du flux des travaux	**4 Flux des travaux de la vérification d'organisation désignée (VOD) pour l'inscription au PSC**
Unité(s) opérationnelle(s)	• Analyste de l'inscription au PSC • Agent d'assurance de la qualité de l'inscription au PSC • Chef de l'inscription au PSC
Objectif opérationnel	• Obtenir une attestation de sécurité pour l'organisation au niveau de l'attestation de sécurité de la VOD
Élément déclencheur	• Nouvelle demande d'inscription ou demande de relèvement • Demande d'inscription CPI ou ADR
Description du flux des travaux	1. Début du processus. 2. L'analyste de l'inscription au PSC confirme que tous les renseignements requis ont été reçus. 3. Dans le cas contraire, l'analyste de l'inscription au PSC détermine s'il est nécessaire de demander les renseignements. Si cela est nécessaire, il communique avec l'organisation. Passez à l'étape 2. Si l'analyste de l'inscription au PSC détermine que le dossier doit être clôturé, passez à l'étape 13. 4. Si tous les renseignements requis ont été reçus, l'analyste de l'inscription au PSC détermine s'il convient de demander un filtrage de sécurité du personnel (FSP). Si aucun filtrage de sécurité du personnel n'est requis, passez à l'étape 9. 5. Si le FSP est requis, l'analyste de l'inscription au PSC crée et envoie une trousse d'inscription à la Division du filtrage de la sécurité du personnel (DFSP) du PSC en demandant des FSP pour les personnes désignées de l'organisation. 6. Le processus de FSP est déclenché (13 FT demande de FSP PSC). 7. La trousse d'inscription est renvoyée par la DFSP et les résultats du FSP sont examinés. 8. En cas de problèmes dans les résultats du FSP, la trousse d'inscription est retournée à la DFSP. Passez à l'étape 5. 9. Si aucun problème n'apparaît dans les résultats du FSP, l'analyste de l'inscription au PSC confirme s'il est nécessaire de résilier l'inscription de l'organisation. S'il n'est pas nécessaire de résilier l'inscription de l'organisation, passez à l'étape 14. 10. S'il s'avère nécessaire de résilier l'inscription de l'organisation, l'analyste de l'inscription au PSC examine l'organisation afin de déterminer s'il existe des éléments pouvant empêcher la résiliation de l'inscription, par exemple si l'organisation est actuellement impliquée dans un contrat actif. S'il existe des éléments pouvant empêcher la résiliation de l'inscription de l'organisation, passez à l'étape 3.

	11. S'il n'existe aucun élément pouvant empêcher la résiliation de l'inscription de l'organisation, toutes les attestations de FSP requises seront résiliées. 12. L'analyste de l'inscription au PSC avise l'agent de sécurité d'entreprise (ASE) et l'organisme parrain de la résiliation. 13. La demande d'inscription est clôturée pour cause de non-conformité. Passez à l'étape 21. 14. L'analyste de l'inscription au PSC crée l'avis d'inscription. 15. Le dossier est présenté à l'agent d'assurance de la qualité du PSC pour examen. 16. L'agent d'assurance de la qualité du PSC examine le dossier. 17. Si l'agent d'assurance de la qualité du PSC détermine que des modifications sont nécessaires, la demande d'inscription est renvoyée à l'analyste de l'inscription au PSC pour qu'il procède à des mises à jour. 18. L'analyste de l'inscription au PSC met le dossier à jour. Passez à l'étape 15. 19. Si l'agent d'assurance de la qualité du PSC estime qu'aucune modification n'est requise, le chef de l'inscription au PSC est invité à signer la lettre d'attribution. 20. L'analyste de l'inscription au PSC avise l'ASE et l'organisme parrain. L'avis contient la lettre d'attestation de l'organisation, les formulaires de breffage de FSP, l'accord sur la sécurité 3G et l'état de sécurité de l'organisation. 21. L'élément déclencheur de la VOD peut déclencher d'autres processus d'inscription. 22. En cas de besoin, l'attestation de sécurité d'installation (ASI) ou l'autorisation de détenir des renseignements (ADR) seront déclenchées. 23. Si nécessaire, le processus de nouvelle inscription ou de mise à jour d'une inscription peut être déclenché (3 Flux de travaux de la nouvelle inscription ou mise à jour de l'inscription au PSC).
Intrants	• Enquête de sécurité sur une organisation du secteur privé (ESOSP) • Lettre d'établissement • Renseignements sur l'organisation fournis • Résultats de la DFSP
Extrants	• Avis de résiliation • Trousse d'inscription à la DFSP • Lettre d'attribution • Lettre d'attestation de l'organisation • Formulaires de breffage du filtrage de sécurité du personnel • Accord sur la sécurité 3G • État de la sécurité de l'organisation

1.1.4.2 Capacité de protection des installations

Identification du flux des travaux	5 Flux des travaux de la capacité de protection des installations (CPI) pour l'inscription au PSC
Unité(s) opérationnelle(s)	• Analyste de l'inscription au PSC • Agent d'assurance de la qualité de l'inscription au PSC • Chef de l'inscription au PSC
Objectif opérationnel	• Obtenir une attestation de sécurité pour l'organisation au niveau de la CPI
Élément déclencheur	• Nouvelle demande d'inscription ou demande de relèvement • Demande d'inscription à la VOD
Description du flux des travaux	1. Début du processus. 2. L'analyste de l'inscription au PSC détermine si l'attestation de sécurité de la VOD doit être traitée. S'il n'est pas nécessaire de traiter une VOD, passez à l'étape 4. 3. S'il s'avère nécessaire de traiter une attestation de sécurité de la VOD, le processus d'attestation de la VOD est déclenché (4 Flux des travaux de la VOD pour l'inscription au PSC) 4. L'analyste de l'inscription au PSC examine l'organisation afin de déceler tout changement ministériel. En l'absence de changement ministériel, passez à l'étape 8. 5. En cas de changement dans l'organisation, l'analyste de l'inscription au PSC examine l'organisation de façon détaillée. 6. L'analyste de l'inscription au PSC tient une réunion d'information avec l'ASE de l'organisation. 7. L'analyste de l'inscription au PSC remplit la partie 1A du rapport sur les exigences. 8. L'analyste de l'inscription au PSC vérifie que tous les renseignements ont été reçus. 9. Dans le cas contraire, l'analyste de l'inscription au PSC détermine s'il est nécessaire de demander les renseignements. Si cela est nécessaire, il communique avec l'organisation. Passez à l'étape 8. Si l'analyste de l'inscription au PSC décide qu'il convient de clôturer le dossier, passez à l'étape 19. 10. Si tous les renseignements requis ont été reçus, l'analyste de l'inscription au PSC détermine s'il convient de demander un filtrage de sécurité du personnel (FSP). Si aucun FSP n'est requis, passez à l'étape 15. 11. Si le FSP est requis, l'analyste de l'inscription au PSC crée et envoie une trousse d'inscription à la Division du filtrage de la sécurité du personnel (DFSP) du PSC en demandant des FSP pour les personnes désignées de l'organisation. 12. Le processus de FSP est déclenché (13 FT demande de FSP PSC). 13. La trousse d'inscription est renvoyée par la DFSP et les résultats du FSP sont examinés. 14. En cas de problèmes dans les résultats du FSP, la trousse d'inscription est retournée à la DFSP. Passez à l'étape 11.

	15. Si aucun problème n'apparaît dans les résultats du FSP, l'analyste de l'inscription au PSC confirme s'il est nécessaire de résilier l'inscription de l'organisation. S'il n'est pas nécessaire de résilier l'inscription de l'organisation, passez à l'étape 20. 16. S'il s'avère nécessaire de résilier l'inscription de l'organisation, l'analyste de l'inscription au PSC examine l'organisation afin de déterminer s'il existe des éléments pouvant empêcher la résiliation de l'inscription, par exemple si l'organisation est actuellement impliquée dans un contrat actif. S'il existe des éléments pouvant empêcher la résiliation de l'inscription de l'organisation, passez à l'étape 9. 17. S'il n'existe aucun élément pouvant empêcher la résiliation de l'inscription de l'organisation, toutes les attestations de FSP requises seront résiliées. 18. L'analyste de l'inscription au PSC avise l'agent de sécurité d'entreprise (ASE) et l'organisme parrain de la résiliation. 19. La demande d'inscription est clôturée pour cause de non-conformité ou l'attestation de sécurité est abaissée au niveau de la VOD. Passez à l'étape 27. 20. L'analyste de l'inscription au PSC crée l'avis d'inscription. 21. Le dossier est présenté à l'agent d'assurance de la qualité du PSC pour examen. 22. L'agent d'assurance de la qualité du PSC examine le dossier. 23. Si l'agent d'assurance de la qualité du PSC détermine que des modifications sont nécessaires, la demande d'inscription est renvoyée à l'analyste de l'inscription au PSC pour qu'il procède à des mises à jour. 24. L'analyste de l'inscription au PSC met le dossier à jour. Passez à l'étape 21. 25. Si l'agent d'assurance de la qualité du PSC estime qu'aucune modification n'est requise, le chef de l'inscription au PSC est invité à signer la lettre d'attribution. 26. L'analyste de l'inscription au PSC avise l'ASE et l'organisme parrain. L'avis contient la lettre d'attestation de l'organisation, les formulaires de breffage de FSP, l'accord sur la sécurité 3G et l'état de sécurité de l'organisation. 27. L'élément déclencheur de la CPI peut déclencher d'autres processus d'inscription. 28. Si besoin, une autorisation de détenir des renseignements (ADR) sera déclenchée (6 Flux des travaux de l'autorisation de détenir des renseignements (ADR) pour l'inscription au PSC). 29. Si nécessaire, le processus de nouvelle inscription ou de mise à jour d'une inscription peut être déclenché (2 Flux de travaux suivant l'attribution du contrat du PSC).
Intrants	• Enquête de sécurité sur une organisation du secteur privé (ESOSP) • Lettre d'établissement • Renseignements sur l'organisation fournis • Résultats de la DFSP
Extrants	• Avis de résiliation • Trousse d'inscription à la DFSP • Lettre d'attribution • Lettre d'attestation de l'organisation • Formulaires de breffage du filtrage de sécurité du personnel • Accord sur la sécurité 3G • État de la sécurité de l'organisation

1.1.4.3 Autorisation de détenir des renseignements

Identification du flux des travaux	6 Flux des travaux de l'autorisation de détenir des renseignements (ADR) pour l'inscription au PSC
Unité(s) opérationnelle(s)	• Analyste de l'inscription au PSC • Directeur de la Direction de la sécurité industrielle canadienne (DSIC)
Objectif opérationnel	• Obtenir une attestation de sécurité pour l'organisation au niveau de l'attestation de sécurité ADR
Élément déclencheur	• Nouvelle demande d'inscription ou demande de relèvement • Demande d'inscription à la VOD
Description du flux des travaux	1. Début du processus. 2. L'analyste de l'inscription au PSC détermine si l'attestation de sécurité de la VOD doit être traitée. S'il n'est pas nécessaire de traiter une VOD, passez à l'étape 4. 3. S'il s'avère nécessaire de traiter une attestation de sécurité de la VOD, le processus d'attestation de la VOD est déclenché (4 Flux des travaux de la VOD pour l'inscription au PSC) 4. L'analyste de l'inscription au PSC détermine si une attestation de sécurité CPI doit être traitée. S'il n'est pas nécessaire de traiter une CPI, passez à l'étape 6. 5. S'il s'avère nécessaire de traiter une attestation de sécurité CPI, le processus d'attestation CPI est déclenché (5 Flux des travaux de la CPI pour l'inscription au PSC) 6. L'analyste de l'inscription au PSC examine l'organisation afin de déceler tout changement ministériel. En l'absence de changement ministériel, passez à l'étape 9. 7. En cas de changement dans l'organisation, l'analyste de l'inscription au PSC examine l'organisation de façon détaillée. 8. L'analyste de l'inscription au PSC tient une réunion d'information avec l'ASE de l'organisation. 9. L'analyste de l'inscription au PSC détermine si l'exclusion de l'organisation mère est requise. Si l'exclusion de l'organisation mère n'est pas requise, passez à l'étape 13. 10. En cas d'exclusion de l'organisation mère, l'analyste du PSC demande des renseignements supplémentaires à l'organisation. 11. L'analyste de l'inscription au PSC examine et analyse les renseignements reçus. 12. Le directeur de la DSIC fournit l'approbation de l'exclusion de l'organisation mère. 13. L'analyste de l'inscription au PSC vérifie que tous les renseignements ont été reçus.

	14. Dans le cas contraire, l'analyste de l'inscription au PSC détermine s'il est nécessaire de demander les renseignements. Si cela est nécessaire, il communique avec l'organisation. Passez à l'étape 13. Si l'analyste de l'inscription au PSC détermine que le dossier doit être clôturé, passez à l'étape 24. 15. Si tous les renseignements requis ont été reçus, l'analyste de l'inscription au PSC détermine s'il convient de demander un filtrage de sécurité du personnel (FSP). Si aucun FSP n'est requis, passez à l'étape 20. 16. Si le FSP est requis, l'analyste de l'inscription au PSC crée et envoie une trousse d'inscription à la Division du filtrage de la sécurité du personnel (DFSP) du PSC en demandant des FSP pour les personnes désignées de l'organisation. 17. Le processus de FSP est déclenché (3 FT demande de FSP PSC). 18. La trousse d'inscription est renvoyée par la DFSP et les résultats du FSP sont examinés. 19. En cas de problèmes dans les résultats du FSP, la trousse d'inscription est retournée à la DFSP. Passez à l'étape 16. 20. Si aucun problème n'apparaît dans les résultats du FSP, l'analyste de l'inscription au PSC confirme s'il est nécessaire de résilier l'inscription de l'organisation. S'il n'est pas nécessaire de mettre fin à l'inscription de l'organisation, passez à l'étape 25. 21. S'il s'avère nécessaire de résilier l'inscription de l'organisation, l'analyste de l'inscription au PSC examine l'organisation afin de déterminer s'il existe des éléments pouvant empêcher la résiliation de l'inscription, par exemple si l'organisation est actuellement impliquée dans un contrat actif. S'il existe des éléments pouvant empêcher la résiliation de l'inscription de l'organisation, passez à l'étape 14. 22. S'il n'existe aucun élément pouvant empêcher la résiliation de l'inscription de l'organisation, toutes les attestations de FSP requises seront résiliées. 23. L'analyste de l'inscription au PSC avise l'agent de sécurité d'entreprise (ASE) et l'organisme parrain de la résiliation. 24. La demande d'inscription est clôturée pour cause de non-conformité. Passez à l'étape 27. 25. L'analyste de l'inscription au PSC crée une demande d'inspection. 26. Le processus d'inspection est déclenché (10 FT de l'inspection du PSC). 27. Si nécessaire, le processus de nouvelle inscription ou de mise à jour d'une inscription peut être déclenché.
Intrants	• Enquête de sécurité sur une organisation du secteur privé (ESOSP) • Lettre d'établissement • Renseignements sur l'organisation fournis • Résultats de la DFSP
Extrants	• Avis de résiliation • Trousse d'inscription à la DFSP • Lettre d'attribution • Lettre d'attestation de l'organisation • Formulaires de breffage du filtrage de sécurité du personnel • Accord sur la sécurité 3G • État de la sécurité de l'organisation

1.1.5 Inscription au Programme de sécurité des contrats (PSC) – Renouvellement

Le processus opérationnel de renouvellement d'une inscription exige de définir et d'aviser les organisations quand leur attestation de sécurité d'organisation arrive à expiration. Les cycles de renouvellement varient selon les types d'attestations de sécurité d'organisation. Les renseignements de renouvellement d'une organisation sont obtenus, examinés et évalués en vue de déterminer si l'organisation a toujours besoin de l'attestation de sécurité d'organisation existante. L'absence de renouvellement de l'attestation de sécurité d'organisation peut entraîner la révocation ou la résiliation.

Identification du flux des travaux	**7 Flux des travaux du renouvellement de l'inscription au PSC**
Unité(s) opérationnelle(s)	• Organisation inscrite • Commis à l'inscription • Analyste de l'inscription au PSC • Agent d'assurance de la qualité de l'inscription au PSC • Chef de l'inscription au PSC
Objectif opérationnel	• Renouveler une attestation de sécurité d'organisation
Élément déclencheur	• Demande de renouvellement d'une organisation
Description du flux des travaux	1. Début du processus. 2. Le commis à l'inscription au PSC publie un rapport sur les organisations arrivant à échéance. 3. Le commis à l'inscription au PSC informe l'organisation des exigences en matière de renouvellement. 4. L'organisation inscrite présente les renseignements de renouvellement. 5. Le commis à l'inscription au PSC examine la demande, établit les priorités et affecte la demande à l'analyste de l'inscription. 6. Le commis à l'inscription au PSC détermine s'il convient de poursuivre le renouvellement. S'il convient de continuer, passez à l'étape 8. 7. S'il n'est pas nécessaire de poursuivre le renouvellement, clôturez la demande pour cause de non-conformité. 8. L'analyste de l'inscription au PSC examine et valide les renseignements de renouvellement. 9. L'analyste de l'inscription au PSC examine l'organisation afin de déceler tout changement ministériel. En l'absence de changement ministériel, passez à l'étape 15. 10. En cas de changement dans l'organisation, l'analyste de l'inscription au PSC examine l'organisation de façon détaillée. 11. L'analyste de l'inscription au PSC détermine s'il existe des exigences en matière d'ADR. En l'absence d'exigences en matière d'ADR, passez à l'étape 14.

	12. L'analyste de l'inscription au PSC présente une demande d'inspection. 13. Le processus d'inspection est déclenché (10 FT de l'inspection du PSC). 14. L'analyste de l'inscription au PSC tient une réunion d'information avec l'ASE de l'organisation. 15. L'analyste de l'inscription au PSC vérifie que tous les renseignements ont été reçus. 16. Dans le cas contraire, l'analyste de l'inscription au PSC détermine s'il est nécessaire de demander les renseignements. Si cela est nécessaire, il communique avec l'organisation. Passez à l'étape 15. Si l'analyste de l'inscription au PSC détermine que le dossier doit être clôturé, passez à l'étape 26. 17. Si tous les renseignements requis ont été reçus, l'analyste de l'inscription au PSC détermine s'il convient de demander un filtrage de sécurité du personnel (FSP). Si aucun FSP n'est requis, passez à l'étape 22. 18. Si le FSP est requis, l'analyste de l'inscription au PSC crée et envoie une trousse d'inscription à la Division du filtrage de la sécurité du personnel (DFSP) du PSC en demandant des FSP pour les personnes désignées de l'organisation. 19. Le processus de FSP est déclenché (13 FT demande de FSP PSC). Passez à l'étape 34. 20. La trousse d'inscription est renvoyée par la DFSP et les résultats du FSP sont examinés. 21. En cas de problèmes dans les résultats du FSP, la trousse d'inscription est retournée à la DFSP. Passez à l'étape 18. 22. Si aucun problème n'apparaît dans les résultats du FSP, l'analyste de l'inscription au PSC confirme s'il est nécessaire de résilier l'inscription de l'organisation. S'il n'est pas nécessaire de résilier l'inscription de l'organisation, passez à l'étape 26. 23. S'il s'avère nécessaire de résilier l'inscription de l'organisation, l'analyste de l'inscription au PSC examine l'organisation afin de déterminer s'il existe des éléments pouvant empêcher la résiliation de l'inscription, par exemple si l'organisation est actuellement impliquée dans un contrat actif. S'il existe des éléments pouvant empêcher la résiliation de l'inscription de l'organisation, passez à l'étape 16. 24. S'il n'existe aucun élément pouvant empêcher la résiliation de l'inscription de l'organisation, toutes les attestations de FSP requises seront résiliées. 25. L'analyste de l'inscription au PSC avise l'agent de sécurité d'entreprise (ASE) et l'organisme parrain de la résiliation. 26. La demande d'inscription est clôturée pour cause de non-conformité ou l'attestation de sécurité est abaissée au niveau de la VOD. Passez à l'étape 34. 27. L'analyste de l'inscription au PSC crée l'avis de renouvellement. 28. Le dossier est présenté à l'agent d'assurance de la qualité du PSC pour examen. 29. L'agent d'assurance de la qualité du PSC examine le dossier. 30. Si l'agent d'assurance de la qualité du PSC détermine que des modifications sont nécessaires, la demande d'inscription est renvoyée à l'analyste de l'inscription au PSC pour qu'il procède à des mises à jour. 31. L'analyste de l'inscription au PSC met le dossier à jour. Passez à l'étape 28. 32. Si l'agent d'assurance de la qualité du PSC estime qu'aucune modification n'est requise, le chef de l'inscription au PSC est invité à signer la lettre d'attribution. 33. L'analyste de l'inscription au PSC avise l'ASE et l'organisme parrain. L'avis contient la lettre d'attestation de l'organisation, les formulaires de breffage de FSP, l'accord sur la sécurité 3G et l'état de sécurité de l'organisation. 34. Fin du processus.

Intrants	• Renseignements de renouvellement • Résultats de la DFSP
Extrants	• Avis de résiliation • Lettre d'attribution • Lettre d'attestation de l'organisation • Formulaires de breffage du filtrage de sécurité du personnel • Accord sur la sécurité 3G • État de la sécurité de l'organisation

1.1.6 Inscription au Programme de sécurité des contrats (PSC) – Mise à jour

Le processus opérationnel de mise à jour d'une inscription exige la présentation de renseignements au PSC de la part de l'organisation aux fins de simplement mettre à jour ses renseignements dans le PSC. Ce processus opérationnel est semblable à celui du renouvellement d'une inscription, sauf que la présentation des renseignements est volontaire. Les renseignements de mise à jour d'une organisation sont obtenus, examinés et évalués en vue de déterminer si l'organisation a toujours besoin de l'attestation de sécurité d'organisation existante. L'absence de renouvellement de l'attestation de sécurité d'organisation peut entraîner la révocation ou la résiliation.

Identification du flux des travaux	**8 Flux des travaux de la mise à jour de l'inscription au PSC**
Unité(s) opérationnelle(s)	• Organisme parrain • Analyste du contrat du PSC • Organisation inscrite • Commis à l'inscription au PSC • Analyste de l'inscription au PSC • Agent d'assurance de la qualité de l'inscription au PSC • Chef de l'inscription au PSC
Objectif opérationnel	• Mettre à jour les renseignements d'une organisation aux fins d'attestation de sécurité

Élément déclencheur	• Demande de mise à jour d'une organisation
Description du flux des travaux	1. Début du processus. 2. L'organisme parrain ou l'analyste du contrat du PSC présente une mise à jour relative à un renseignement de l'organisation. 3. L'organisation inscrite présente une mise à jour de ses renseignements. 4. Le commis à l'inscription au PSC examine la demande, établit les priorités et affecte la demande à l'analyste de l'inscription. 5. Le commis à l'inscription au PSC détermine s'il convient de poursuivre la mise à jour. S'il convient de continuer, passez à l'étape 8. 6. S'il n'est pas nécessaire de poursuivre la mise à jour, rejetez la demande de mise à jour. 7. Le commis à l'inscription au PSC avise l'ASE du rejet de la mise à jour. Passez à l'étape 34. 8. L'analyste de l'inscription au PSC examine et valide les renseignements de mise à jour. 9. L'analyste de l'inscription au PSC examine l'organisation afin de déceler tout changement ministériel. En l'absence de changement ministériel, passez à l'étape 15. 10. En cas de changement dans l'organisation, l'analyste de l'inscription au PSC examine l'organisation de façon détaillée. 11. L'analyste de l'inscription au PSC détermine s'il existe des exigences en matière d'ADR. En l'absence d'exigences en matière d'ADR, passez à l'étape 14. 12. L'analyste de l'inscription au PSC présente une demande d'inspection. 13. Le processus d'inspection est déclenché (10 FT de l'inspection du PSC). Passez à l'étape 34. 14. L'analyste de l'inscription au PSC tient une réunion d'information avec l'ASE de l'organisation. 15. L'analyste de l'inscription au PSC vérifie que tous les renseignements ont été reçus. 16. Dans le cas contraire, l'analyste de l'inscription au PSC détermine s'il est nécessaire de demander les renseignements. Si cela est nécessaire, il communique avec l'organisation. Passez à l'étape 15. Si l'analyste de l'inscription au PSC détermine que le dossier doit être clôturé, passez à l'étape 26. 17. Si tous les renseignements requis ont été reçus, l'analyste de l'inscription au PSC détermine s'il convient de demander un filtrage de sécurité du personnel (FSP). Si aucun FSP n'est requis, passez à l'étape 22. 18. Si le FSP est requis, l'analyste de l'inscription au PSC crée et envoie une trousse d'inscription à la Division du filtrage de la sécurité du personnel (DFSP) du PSC en demandant des FSP pour les personnes désignées de l'organisation. 19. Le processus de FSP est déclenché (13 FT demande de FSP PSC). 20. La trousse d'inscription est renvoyée par la DFSP et les résultats du FSP sont examinés. 21. En cas de problèmes dans les résultats du FSP, la trousse d'inscription est retournée à la DFSP. Passez à l'étape 18. 22. Si aucun problème n'apparaît dans les résultats du FSP, l'analyste de l'inscription au PSC confirme s'il est nécessaire de résilier l'inscription de l'organisation. S'il n'est pas nécessaire de résilier l'inscription de l'organisation, passez à l'étape 27. 23. S'il s'avère nécessaire de résilier l'inscription de l'organisation, l'analyste de l'inscription au PSC examine l'organisation afin de déterminer s'il existe des éléments pouvant empêcher la résiliation de l'inscription, par exemple si l'organisation est actuellement impliquée dans un contrat actif. S'il existe des éléments pouvant empêcher la résiliation de l'inscription de l'organisation, passez à l'étape 16.

	24. S'il n'existe aucun élément pouvant empêcher la résiliation de l'inscription de l'organisation, toutes les attestations de FSP requises seront résiliées. 25. L'analyste de l'inscription au PSC avise l'agent de sécurité d'entreprise (ASE) et l'organisme parrain de la résiliation. 26. La demande d'inscription est clôturée pour cause de non-conformité. Passez à l'étape 34. 27. L'analyste de l'inscription au PSC met à jour les renseignements de l'organisation. 28. Le dossier est présenté à l'agent d'assurance de la qualité du PSC pour examen. 29. L'agent d'assurance de la qualité du PSC examine le dossier. 30. Si l'agent d'assurance de la qualité du PSC détermine que des modifications sont nécessaires, la demande d'inscription est renvoyée à l'analyste de l'inscription au PSC pour qu'il procède à des mises à jour. 31. L'analyste de l'inscription au PSC met le dossier à jour. Passez à l'étape 28. 32. Si l'agent d'assurance de la qualité du PSC estime qu'aucune modification n'est requise, le chef de l'inscription au PSC est invité à signer la lettre d'attribution. 33. L'analyste de l'inscription au PSC avise l'ASE et l'organisme parrain. L'avis contient la lettre d'attestation de l'organisation, les formulaires de breffage de FSP, l'accord sur la sécurité 3G et l'état de sécurité de l'organisation. 34. Fin du processus.
Intrants	• Renseignements de mise à jour • Résultats de la DFSP
Extrants	• Avis de résiliation • Lettre d'attribution • Lettre d'attestation de l'organisation • Formulaires de breffage du filtrage de sécurité du personnel • Accord sur la sécurité 3G • État de la sécurité de l'organisation

1.1.7 Inscription au Programme de sécurité des contrats (PSC) – Résiliation

Le processus opérationnel de résiliation d'une inscription englobe la réception d'une demande de résiliation d'une organisation, l'examen et l'évaluation de la demande de résiliation, la résiliation des attestations de sécurité de l'organisation et de son personnel, et enfin un communiqué informant l'organisation de la résiliation. Les demandes de résiliation peuvent être présentées par l'organisme parrain, par l'organisation elle-même ou par le PSC. Les demandes de résiliation reçues font d'abord l'objet d'un examen afin de déterminer s'il existe des éléments pouvant empêcher la résiliation, par exemple un contrat en cours ou le fait que l'organisation avait une attestation de sécurité ADR et que les documents étaient stocké sur place.

Identification du flux des travaux	9 Flux des travaux de la résiliation de l'inscription au PSC
Unité(s) opérationnelle(s)	• Organisme parrain • Organisation inscrite • Analyste de l'inscription au PSC
Objectif opérationnel	• Résilier une attestation de sécurité d'organisation
Élément déclencheur	• Demande de résiliation d'une organisation
Description du flux des travaux	1. Début du processus. 2. L'organisme parrain présente une demande de résiliation de l'organisation qu'il parraine. 3. Autre début du processus. 4. L'organisation inscrite présente une demande de résiliation de son organisation. 5. Autre début du processus. 6. Le commis à l'inscription au PSC présente une demande de résiliation d'une organisation. 7. L'analyste de l'inscription au PSC examine les renseignements et analyse la demande de résiliation. 8. L'analyste de l'inscription au PSC détermine s'il existe des exigences en matière d'ADR. En l'absence d'exigences en matière d'ADR, passez à l'étape 9. 9. L'analyste de l'inscription au PSC présente une demande d'inspection. 10. Le processus d'inspection est déclenché (10 FT de l'inspection du PSC). Passez à l'étape 14. 11. L'analyste de l'inscription au PSC résilie l'inscription de l'organisation. 12. L'analyste de l'inscription au PSC résilie toutes les demandes de filtrage de sécurité du personnel. 13. L'analyste de l'inscription au PSC avise l'ASE et l'organisme parrain de la résiliation. 14. Fin du processus.
Intrants	• Demande de résiliation
Extrants	• Demande de résiliation de l'organisation

1.1.8 Inscription au Programme de sécurité des contrats (PSC) – Inspection

Le processus opérationnel de l'inspection dans le cadre de l'inscription effectue des examens de sécurité physique et informatique des organisations pour assurer la vérification et le respect des exigences relatives à la sécurité industrielle de l'organisation, des exigences relatives à la sécurité de la technologie de l'information, des niveaux d'Autorisation de détenir des renseignements (ADR) appropriés, de l'harmonisation des renseignements relatifs à l'entreprise et au contrat, au besoin et pour fournir des conseils et des directives aux agents de sécurité d'entreprise (ASE).

Identification du flux des travaux	**10 Inspection du flux des travaux du PSC**
Unité(s) opérationnelle(s)	• Représentant de l'organisation • Inspecteur du PSC • Inspecteur principal du PSC • Gestionnaire d'inspection du PSC • Inscription au PSC/Contrats du PSC
Objectif opérationnel	• Effectuer des examens de sécurité physique et de technologie d'information (TI) d'une organisation pour assurer la vérification et le respect des éléments suivants : o les organisations sont conformes aux exigences relatives à la sécurité industrielle; o les exigences relatives à la sécurité de la TI sont respectées; o le niveau d'ADR est approprié; o l'harmonisation des renseignements relatifs à l'entreprise et au contrat est assurée en veillant à ce que tous les renseignements répondent aux normes de qualité établies; o la fourniture de conseils et des directives aux ASE au sujet des exigences en matière de sécurité.
Élément déclencheur	• Divers éléments déclencheurs provenant des autres flux de travail.
Description du flux des travaux	1. Début du processus. 2. Flux de travail lié à l'inscription (3 Flux de travail lié à l'inscription). 3. Flux de travail après l'attribution du contrat (2 Flux de travail après l'attribution du contrat). 4. Renouvellement de l'ADR. Consulter le dernier point dans la section des éléments déclencheurs ci-dessus. (6 Flux des travaux de l'autorisation de détenir des renseignements (ADR) pour l'inscription au PSC). 5. L'inspecteur principal examine la demande d'inspection. 6. Décision : La documentation relative à la demande d'inspection est-elle complète? [Oui : étape 8; Non : étape 6]. 7. La demande de l'inspecteur principal comporte des renseignements manquants du demandeur, qui pourraient provenir de la division de l'inscription ou des contrats.

	8. L'analyse des inscriptions ou le spécialiste des contrats fournit les renseignements manquants relatifs à l'inspection à l'inspecteur principal. 9. L'inspecteur principal détermine si l'inspection doit avoir lieu sur place (cela s'applique aux inspections physiques et de TI) ou peut être effectuée hors site (lorsqu'il faut procéder seulement à une entrevue téléphonique). 10. L'inspecteur principal détermine quel inspecteur devrait être affecté à la demande selon la région, la disponibilité et l'expertise de l'inspecteur. 11. L'inspecteur principal attribue la demande d'inspection à l'inspecteur. 12. Décision. L'organisation a-t-elle été inspectée il y a moins d'un an? [Oui : étape 12; Non : étape 18]. 13. L'inspecteur communique avec le représentant de l'organisation pour confirmer si des changements ont été apportés depuis la dernière inspection. 14. Décision. Des changements ont-ils été apportés depuis la dernière inspection? [Oui : étape 19; Non : étape 14]. 15. L'inspecteur prépare le rapport d'inspection et le soumet à l'inspecteur principal. Ce rapport indiquera qu'aucun changement n'a été apporté depuis la dernière inspection. L'organisation respecte l'exigence de l'ADR/l'attestation de sécurité d'installation (ASI) pour le contrat. S'il existe une exigence en matière de TI pour le contrat, l'inspecteur inclura dans le rapport une recommandation visant à examiner l'exigence en matière de TI. 16. L'inspecteur principal examinera le rapport d'inspection, ainsi que la recommandation. 17. Décision. Un examen d'inspection de la TI est-il nécessaire? [Oui : étape 17; Non : étape 18]. 18. L'inspecteur principal attribue l'inspection de la TI à un spécialiste d'inspection de la TI. 19. L'inspecteur établit la première communication avec le représentant de l'organisation par courriel ou par téléphone. Cette première communication vise à ce que l'inspecteur se présente et décrive le processus d'inspection. 20. Décision. L'organisation doit-elle remplir une demande d'ADR? [Oui : étape 20; Non : étape 31]. La demande d'ADR a été envoyée à l'organisation lorsque l'inspection sera menée hors site, ou si le contrat comprenait la TI. 21. L'inspecteur envoie un dossier de la demande d'ADR au représentant de l'organisation (client). Un délai de 30 jours ouvrables est accordé à l'organisation pour saisir et soumettre ces renseignements. 22. L'organisation a fourni des renseignements au PSC. 23. Décision. Le client a-t-il fourni des renseignements relatifs à l'ADR dans les dix premiers jours suivant la réception de l'avis du PSC? [Oui : étape 29; Non : étape 23]. 24. Un avis de suivi a été envoyé au représentant de l'organisation pour rappeler que l'inspecteur doit recevoir des renseignements pour procéder à l'inspection. 25. Décision. Le client a-t-il fourni des renseignements relatifs à l'ADR dans les vingt premiers jours suivant la réception de l'avis du PSC? [Oui : étape 29; Non : étape 24].

	26. Un deuxième avis de suivi a été envoyé au représentant de l'organisation pour rappeler qu'il doit fournir les renseignements exigés pour procéder à l'inspection. 27. Décision. Le client a-t-il fourni les renseignements relatifs à l'ADR dans les 25 jours suivant la réception de l'avis de retard? [Oui : étape 29; Non : étape 27]. 28. L'avis de suivi final demandant l'achèvement et la soumission du dossier de renseignements relatifs à l'ADR est envoyé au représentant de l'organisation. L'organisation doit fournir les renseignements demandés dans les cinq prochains jours. Une copie conforme de cet avis est envoyée à l'autorité contractante. 29. Décision. Le client a-t-il fourni les renseignements relatifs à l'ADR dans un délai de 30 jours? [Oui : étape 29; Non : étape 45]. 30. Décision. L'inspecteur recommande-t-il d'effectuer une inspection sur place plutôt que hors site? [Oui : étape 30; Non : étape 32]. 31. L'inspecteur principal approuve la recommandation de l'inspecteur visant à mener plutôt une inspection sur place. 32. L'inspecteur envoie une demande de renseignements au représentant de l'organisation. Le client peut fournir ces renseignements avant que l'inspecteur se rende sur le site de l'organisation pour mener l'inspection. Les renseignements demandés facilitent la préparation de l'inspection. 33. L'inspecteur recueille tous les renseignements fournis pour cette inspection. 34. L'inspecteur se prépare en vue de l'inspection. 35. L'inspecteur fixe la date de l'inspection. 36. L'inspecteur mène l'inspection. Dans le cas d'une inspection sur place, cette étape comprendrait le déplacement de l'inspecteur vers le site de l'organisation à inspecter. 37. L'inspecteur prépare le rapport de l'inspection. Dans le cas où le site de l'organisation échoue l'inspection, l'inspecteur inclura dans le rapport les recommandations pour l'organisation. 38. L'inspecteur principal examine le rapport et apporte des modifications, s'il y a lieu; cela peut comprendre des modifications aux recommandations. 39. Le gestionnaire examinera et signera le rapport/les recommandations. 40. Décision. L'organisation est-elle conforme? [Oui : étape 40; Non : étape 42]. 41. L'inspecteur envoie l'avis de conformité au représentant de l'organisation et à l'une ou l'autre des parties intéressées du Secteur de la sécurité industrielle (SSI) ou à au moins la division qui a déclenché l'inspection. 42. L'inspecteur clôt la demande d'inspection. 43. Fin du processus 44. L'inspecteur envoie un avis dans les 30 jours ouvrables au représentant de l'organisation. L'avis décrira les recommandations que l'organisation doit mettre en œuvre dans son site aux fins de conformité. Elle doit le faire selon le délai fixé. 45. Mettre en place le processus non conforme à l'inspection (11 Inspection du flux des travaux du PSC non conforme). 46. Décision. L'organisation est-elle conforme? [Oui : étape 40; Non : étape 41]. 47. L'inspecteur envoie un avis au demandeur, qui explique que l'inspection ne sera pas effectuée, puisque le client n'a pas envoyé les renseignements demandés dans un délai de 30 jours ouvrables. La demande d'inspection doit être soumise de nouveau.

	48. L'inspecteur remplit le rapport d'inspection dans le cas où le client n'a pas fourni les renseignements relatifs à l'ADR comme il a été demandé.
Intrants	• S.O.
Extrants	• Rapport et recommandation • Lettre d'approbation • Lettre/avis visant à informer l'organisation qu'elle n'a pas obtenu l'ADR demandée. • Lettre de non-conformité

1.1.9 Inscription au PSC – Inspection non conforme

Identification du flux des travaux	**11 Inspection du flux des travaux du PSC non conforme**
Unité(s) opérationnelle(s)	• Représentant de l'organisation • Inspecteur du PSC
Objectif opérationnel	• Effectuer des examens de sécurité physique et de technologie d'information (TI) d'une organisation pour assurer la vérification des éléments suivants : o les organisations sont conformes aux exigences relatives à la sécurité industrielle; o les exigences relatives à la sécurité de la TI sont respectées; o le niveau d'ADR est approprié; o l'harmonisation des renseignements relatifs à l'entreprise et au contrat est assurée en veillant à ce que tous les renseignements répondent aux normes de qualité établies; o la fourniture de conseils et des directives aux ASE au sujet des exigences en matière de sécurité.
Élément déclencheur	• Processus d'inspection : lorsqu'on envoie un avis dans les 30 jours à une organisation pour mettre en œuvre des recommandations afin que son site réussisse l'ADR/l'ASI ou l'inspection de TI.
Description du flux des travaux	1. Début du processus 2. Un avis peut être reçu du représentant de l'organisation pour informer le SSI que les recommandations proposées ont été mises en œuvre. La ligne pointillée est utilisée pour indiquer si un événement peut ou non se produire. 3. Décision. Les recommandations ont-elles été mises en œuvre dans le délai prescrit de 30 jours? [Oui : étape 4; Non : étape 7]. 4. L'inspecteur effectue l'inspection de suivi. Cette inspection pourrait avoir lieu sur place ou hors site. 5. Décision. L'inspection a-t-elle été réussie? [Oui : 6; Non : 7]

	6. Fin du processus. Retourner au flux de travail de l'inspection. 7. Décision. L'inspection visait-elle un nouveau site d'ADR? [Oui : étape 8; Non : étape 9]. 8. L'inspecteur prépare et envoie l'avis selon lequel le site de l'organisation n'obtient pas l'ADR demandée. 9. L'inspecteur dote l'organisation du statut de non-conformité. 10. Décision. Y a-t-il un contrat en cours avec cette organisation dans le site en question? [Oui : étape 16; Non : étape 11]. 11. L'inspecteur accorde un délai supplémentaire à l'organisation pour mettre en œuvre les recommandations. Le délai est fixé selon la situation de l'organisation et les recommandations qui doit être mises en œuvre. Il peut varier de 5 à 45 jours. 12. Décision. Les recommandations ont-elles été mises en œuvre dans le délai supplémentaire? [Oui : étape 13; Non : étape 15]. 13. L'inspecteur effectue l'inspection de suivi. Cette inspection pourrait avoir lieu sur place ou hors site. 14. Décision. L'inspection a-t-elle été réussie? [Oui : 6; Non : 15] 15. L'inspecteur prépare l'avis de non-conformité et l'envoie à l'organisation et aux parties intéressées du SSI, particulièrement à la division qui a déclenché l'inspection au début du processus. 16. Mettre en place le processus de la Politique ministérielle 123. Il s'agit de la conformité et la mise en application des exigences relatives à la sécurité industrielle. 17. Fin du processus.
Intrants	• S.O.
Extrants	• Lettre/avis visant à informer l'organisation qu'elle n'a pas obtenu l'ADR demandée. • Lettre de non-conformité

1.1.10 Inscription au PSC – Enquête

Le processus opérationnel d'enquête de l'organisation effectue une enquête sur des cas signalés d'atteintes à la sécurité des contrats soupçonnées. Les enquêteurs rassemblent et examinent les renseignements organisationnels, ainsi que les renseignements concernant la demande d'enquête. Au besoin, un examen approfondi est effectué avant de mener l'enquête. Un rapport est produit à la suite de l'enquête, qui comprend des recommandations sur la meilleure façon de gérer l'incident de sécurité. Au besoin, les autres divisions dans le PSC, les autres ministères du gouvernement du Canada ou les responsables des politiques sont avisés de l'incident de sécurité.

Identification du flux des travaux	**12 Inspection du flux des travaux du PSC – Enquête**
Unité(s) opérationnelle(s)	• Inspecteur du PSC (agent régional de la sécurité industrielle [ARSI]) • Inspecteur principal du PSC (ARSI principal) • Gestionnaire d'inspection du PSC (gestionnaire de l'ARSI)

	• Directeur de la Direction de la sécurité industrielle canadienne (DSIC)
Objectif opérationnel	• Effectuer des enquêtes, au besoin.
Élément déclencheur	• Divers éléments déclencheurs provenant des autres flux de travail liés à l'inscription.
Description du flux des travaux	1. Début du processus. 2. L'inspecteur principal du PSC effectue un examen préliminaire de l'allégation ou de la demande d'enquête. 3. L'inspecteur principal du PSC détermine si l'enquête fait partie du mandat de la Division des inspections et des enquêtes (DIE). Si l'enquête ne relève pas du mandat de la DIE, passez à l'étape 39. 4. Si l'enquête relève du mandat de la DIE, l'inspecteur principal du PSC mène une évaluation des risques et donne un degré de priorité élevée à la demande d'enquête. 5. Le gestionnaire des enquêtes du PSC examine l'évaluation des risques. 6. L'inspecteur principal du PSC attribue l'enquête à un inspecteur selon les risques de l'enquête et l'expérience de l'inspecteur. 7. L'inspecteur du PSC recueille des renseignements supplémentaires et se prépare en vue de l'enquête. 8. L'inspecteur du PSC réalise une enquête préliminaire. 9. L'inspecteur du PSC détermine si l'enquête est requise. Si aucune enquête n'est requise, passez à l'étape 39. 10. Si l'enquête est requise, l'inspecteur du PSC communiquera avec l'ASE de l'organisation pour l'informer de l'enquête. 11. L'inspecteur du PSC crée le plan d'enquête pour l'assurance de la qualité et le soumet à l'inspecteur principal du PSC. 12. L'inspecteur principal du PSC ou le gestionnaire d'inspection du PSC approuve le plan d'enquête pour l'assurance de la qualité. 13. Si l'enquête n'est pas considérée comme à haut risque à l'étape 4, passez à l'étape 15. 14. Si l'enquête est considérée comme à haut risque à l'étape 4, le plan d'enquête est soumis au directeur de la DSIC aux fins d'examen et d'approbation. 15. L'inspecteur du PSC mène l'enquête et détermine s'il existe un « motif valable » pour les personnes concernées par l'enquête. S'il existe un « motif valable », la personne est déclarée à l'unité responsable des enquêtes sur la sécurité (URES) pour un entretien individuel. Si le processus du 22 flux des travaux du PSC de l'URES est déclenché, passez à l'étape 16. 16. L'inspecteur du PSC mène une analyse des conclusions de l'enquête et détermine des mesures correctives. 17. L'inspecteur du PSC crée un rapport comportant des recommandations visant à apporter des corrections. 18. L'inspecteur principal du PSC ou le gestionnaire d'inspection du PSC examine le rapport et les recommandations. 19. Le gestionnaire d'inspection du PSC détermine s'il est nécessaire de disposer d'une lettre d'avertissement ou s'il y aura une couverture médiatique. Si non, passez à l'étape 21. 20. S'il est nécessaire de disposer d'une lettre d'avertissement ou s'il y aura une couverture médiatique, le directeur de la DSIC examine le rapport et les recommandations. 21. L'inspecteur du PSC avise les autres divisions, au besoin.

	22. L'inspecteur du PSC détermine si les allégations sont confirmées. Si les allégations ne sont pas confirmées, passez à l'étape 37. 23. Si les allégations sont confirmées, l'inspecteur du PSC déclare toute activité criminelle soupçonnée au service de police. 24. L'inspecteur du PSC avise l'autorité contractante et l'entrepreneur principal. 25. Si le rapport présentait des mesures correctrices, passez à l'étape 26. S'il n'y avait pas de mesures correctrices, passez à l'étape 35. 26. L'inspecteur du PSC entame le processus de la Politique ministérielle 123. 27. En raison du processus de la Politique ministérielle 123, l'inspecteur du PSC détermine si une révocation immédiate doit être prononcée. 28. Si une révocation immédiate doit être prononcée, l'inspecteur du PSC prépare la lettre de révocation, qui doit être envoyée à l'ASE et à l'autorité contractante. 29. La lettre de révocation est signée par le directeur, puis envoyée. 30. L'inspecteur du PSC détermine s'il existe une incidence sur les employés de l'organisation. S'il n'y a pas d'incidence, passez à l'étape 32. 31. S'il y a une incidence sur les employés de l'organisation, le processus de l'URES est déclenché (22 flux des travaux du PSC de l'URES). 32. L'inspecteur du PSC met fin au contrat de l'organisation. 33. L'inspecteur du PSC poursuit le processus de la Politique ministérielle 123, passez à l'étape 42. 34. Si l'enquête ne relève pas du mandat de la DIE, l'inspecteur principal du PSC ou l'inspecteur du PSC préparera un rapport. 35. L'inspecteur principal du PSC ou l'inspecteur du PSC, s'il y a lieu, avisera les autres divisions au sein du Programme de la sécurité industrielle (PSI) et des autres organisations gouvernementales. 36. Un suivi est prévu au besoin. 37. L'inspecteur du PSC mène le suivi. Passez à l'étape 42. 38. Si aucune allégation n'est confirmée, l'inspecteur du PSC prépare un rapport. 39. L'inspecteur du PSC, s'il y a lieu, avisera les autres divisions au sein du PSI et des autres organisations gouvernementales. Passez à l'étape 42. 40. Si aucune mesure corrective n'est nécessaire, le gestionnaire d'inspection du PSC envoie une lettre de mise en garde à l'ASE. 41. Le gestionnaire d'inspection du PSC demande un accusé-réception des lettres. 42. L'inspecteur principal du PSC clôt l'enquête. 43. Fin du processus.
Intrants	• S.O.
Extrants	• Résultats de l'enquête.

1.1.11 Demande d'attestation de sécurité du personnel

La fonction administrative de Service de filtrage de sécurité du personnel a pour objet de fournir des services de filtrage de sécurité du personnel aux employés d'organisations du secteur privé canadien inscrits au Programme de sécurité des contrats (PSC) qui participent à des contrats visés par des exigences de sécurité ainsi qu'aux employés d'autres ministères du gouvernement du Canada, sur demande. Le filtrage de sécurité du personnel permet de s'assurer que les employés qui participent à des contrats visés par des exigences de sécurité ont un niveau d'accès compatible avec leur besoin de savoir et font preuve de fiabilité et de loyauté envers le Canada, conformément aux exigences du niveau de sécurité approprié qui est défini dans le contrat, avant d'accéder à des renseignements, à des biens ou à des lieux de travail protégés ou classifiés. Dans le cadre du filtrage de sécurité, le PSC recueillera des renseignements auprès de ses partenaires de sécurité afin d'effectuer le filtrage de sécurité nécessaire pour déterminer la fiabilité et la loyauté d'employés envers le Canada.

Le processus administratif de traitement des demandes d'attestation de sécurité du personnel comprend la réception des demandes et la vérification de leur exhaustivité et de l'exactitude des informations qui y figurent, avant de les traiter. Cette vérification est effectuée en comparant les renseignements figurant dans la nouvelle demande avec ceux qui figurent dans les demandes existantes, le cas échéant, afin de rechercher les changements ou les incohérences éventuels. Les demandes d'attestation seront rejetées pour non-conformité, si les personnes visées par les demandes sont incapables de fournir tous les renseignements requis. Seul l'agent de sécurité d'entreprise (ASE) qui a été désigné par une organisation peut soumettre une demande d'attestation de sécurité du personnel (ASP) au PSC.

Identification du flux des travaux	**13 FT demande de FSP PSC**
Unité(s) opérationnelle(s)	• Agent de sécurité de l'organisation • Individu (demandeur) • Inscription au PSC • Spécialiste du filtrage du PSC
Objectif opérationnel	• Réception et priorisation des demandes de FSP
Élément déclencheur	• Demande de FSP soumise par une organisation • Inscription de l'organisation au PSC • Demande d'ASP créée par la Division de filtrage de la sécurité du personnel (DFSP) du PSC
Description du flux des travaux	1. Début du processus 2. L'ASE crée une demande de FSP d'un employé de son organisation. 3. Le demandeur remplit la demande de FSP

	4. L'ASE soumet la demande de FSP 5. Lors de l'inscription de l'organisation auprès du PSC, une trousse de FSP est créée. 6. La trousse de FSP de l'inscription au PSC est transférée à la Division de filtrage de la sécurité du personnel (DFSP). 7. Dans certains cas, le PSC de la DFSP a créé des demandes d'ASP. 8. Le PSC de la DFSP crée les demandes d'ASP en réponse aux demandes externes reçues par courrier, par télécopieur ou par courriel. 9. Le spécialiste du filtrage du PSC vérifie s'il s'agit d'une demande de résiliation Si oui, passez à l'étape 29. 10. Si non, le spécialiste du filtrage du PSC examine la demande et vérifie l'exhaustivité et l'exactitude des renseignements qui y figurent. 11. S'il n'y a pas de problèmes avec les renseignements, passez à l'étape 14. 12. S'il y a des problèmes avec les renseignements, le spécialiste du filtrage du PSC déterminera s'il faut demander au demandeur de fournir des renseignements supplémentaires. Si oui, le spécialiste du filtrage du PSC soumettra une demande de renseignements supplémentaires. Passez à l'étape 10. 13. Si non, le spécialiste du filtrage du PSC fermera la demande et retournera tout document original aux agents de la sécurité. Passez à l'étape 30. 14. Si la demande qui a été reçue doit être saisie manuellement dans le système administratif de la DFSP, le spécialiste du filtrage du PSC se charge d'effectuer la saisie des données. 15. Selon la nature de la demande, l'un des sous-procédés suivants sera déclenché. Si la demande vise une nouvelle ASP, le nouveau sous-processus est déclenché. 16. Le processus de traitement d'une nouvelle ASP est déclenché. (14 FT nouvelle demande de FSP PSC) 17. S'il s'agit d'une demande de mise à jour d'une ASP existante, 18. le processus de traitement d'une mise à jour d'une ASP est déclenché. (15 FT mise à jour d'une demande de FSP PSC) 19. Si la demande vise le relèvement d'une ASP existante 20. Le processus de traitement d'un relèvement d'une ASP est déclenché. (16 FT mise à jour d'une demande de FSP PSC) 21. Si la demande vise le transfert d'une ASP d'une organisation à une autre. 22. Le processus de traitement d'un transfert de l'ASP est déclenché. (17 FT transfert d'une demande de FSP PSC) 23. Si la demande est un double d'une ASP existante. 24. Le processus de traitement d'un double d'une ASP est déclenché. (18 FT duplication d'une demande de FSP PSC) 25. Si la demande vise la réactivation d'une ASP. 26. Le processus de traitement d'une réactivation d'une ASP est déclenché. (19 FT réactivation d'une demande de FSP PSC) 27. Si la demande porte sur une attestation de l'OTAN/COSMIC. 28. Le processus d'attestation de l'OTAN/COSMIQUE est déclenché. (21 FT attestation OTAN PSC). 29. Le processus de résiliation d'une attestation est déclenché (20 FT résiliation d'une demande de FSP PSC) 30. Fin du processus
Intrants	• Demande d'ASP

Extrants	• Fermeture d'une demande d'ASP • Déclenchement de n'importe quel des divers processus de la DFSP

1.1.12 Attestation de sécurité du personnel – nouveau

Le processus administratif de FSP consiste à évaluer le personnel en fonction du niveau de sécurité précisé dans les exigences de sécurité énoncées dans les contrats. Le filtrage de sécurité du personnel vise à vérifier le besoin de savoir, les antécédents, le casier judiciaire, les empreintes digitales et le crédit, ainsi qu'à effectuer une vérification des documents sur le respect de la loi, une vérification hors frontières, des enquêtes de sources ouvertes, des vérifications des antécédents effectuées par le Service canadien du renseignement de sécurité (SCRS) et des tests polygraphiques, selon le niveau d'attestation requis. Le personnel qui est réputé être fiable et loyal envers le Canada se voit accorder l'un des types suivants d'ASP :

a. cote de fiabilité
b. cote d'accès aux sites
c. cote de fiabilité approfondie
d. cote de sécurité de niveau « Secret »
e. OTAN et COSMIC
f. autorisation d'accès au site
g. autorisation de sécurité de niveau Très secret
h. autorisation de sécurité du SIGNIT de niveau très secret
i. autorisation de sécurité de fiabilité approfondie de niveau très secret

Les personnes jugées comme ayant une bonne réputation sont accordées une attestation de sécurité et peuvent désormais avoir accès à des renseignements et à des biens protégés ou classifiés du GC pour accomplir leur travail. Le dossier des personnes dont l'analyse d'attestation donne des résultats négatifs est transmis à l'Unité responsable des enquêtes de sécurité pour traitement afin de dissiper tout doute qui pourrait subsister. À ce stade, une personne sera accordée une ASP demandée ou son dossier de demande sera fermé pour non-conformité.

Une autorisation d'accès aux sites est requise pour permettre au personnel de pénétrer dans des installations sensibles du GC, mais ne permet pas l'accès à des renseignements ou à des biens de nature délicate.

Il faut un certificat spécial d'enquête de sécurité et un profil de sécurité de l'OTAN, avant d'obtenir une ASP donnant l'autorisation d'échanger des renseignements ou de biens avec les pays partenaires de l'OTAN. Tous les citoyens canadiens sont admissibles à une cote de sécurité de l'OTAN accordée par le Canada. Toutefois, les citoyens des autres pays ne sont admissibles qu'à la cote de sécurité accordée par leur pays.

Identification du flux des travaux	14 FT nouvelle demande de FSP PSC
Unité(s) opérationnelle(s)	• Spécialiste du filtrage du PSC
Objectif opérationnel	• Traitement d'une nouvelle demande d'ASP
Élément déclencheur	• Demande d'une nouvelle ASP
Description du flux des travaux	1. Début du processus 2. Pour les demandes de cote de fiabilité et d'accès aux sites, le spécialiste du filtrage du PSC déclenche les vérifications de correspondance du numéro de contrôle du document (NCD) d'empreintes digitales, en examinant si le NCD figurant dans la demande correspond à un ensemble de résultats d'empreintes digitales de la GRC. 3. Le spécialiste du filtrage du PSC effectuera une vérification du crédit de la personne. 4. Le spécialiste du filtrage du PSC déterminera s'il faut effectuer une vérification hors pays. Si aucune vérification hors pays n'est requise, passez à l'étape 6. 5. Si une vérification hors pays est requise, le processus de vérification hors pays est déclenché (FT hors pays FSP PSC). 6. Le spécialiste du filtrage du PSC analyse les résultats de la vérification des empreintes digitales, de la vérification du crédit et de la vérification hors pays. 7. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 11. 8. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 11. 9. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). 10. Si aucun traitement supplémentaire n'est requis, passez à l'étape 50. 11. Si la demande exige une cote de fiabilité approfondie, continuez; si non, passez à l'étape 20. 12. Pour établir une cote de fiabilité approfondie, le spécialiste du filtrage du PSC déclenchera les vérifications de sécurité suivantes : vérification des documents sur le respect de la loi. 13. Le spécialiste du filtrage de sécurité du personnel demandera que la personne remplisse un questionnaire sur la sécurité ou passe une entrevue sur la sécurité. 14. Le spécialiste du filtrage de sécurité du personnel effectuera une enquête de sources ouvertes de la personne. 15. Le spécialiste du filtrage de sécurité du personnel analyse les résultats de la vérification des documents sur le respect de la loi, du questionnaire/entrevue sur la sécurité et de l'enquête de sources ouvertes.

	16. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 20. 17. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 20. 18. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). 19. Si aucun traitement supplémentaire n'est requis, passez à l'étape 50. 20. Si la demande exige une autorisation de sécurité de niveau secret et d'accès aux sites, continuez; si non, passez à l'étape 27. 21. Dans le cas des autorisations de sécurité de niveau secret et d'accès aux sites, le spécialiste du filtrage de sécurité du personnel déclenchera une évaluation de la sécurité par le SCRS. 22. Le spécialiste du filtrage de sécurité du personnel analyse les résultats de l'évaluation de la sécurité par le SCRS. 23. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 27. 24. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 27. 25. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). 26. Si aucun traitement supplémentaire n'est requis, passez à l'étape 50. 27. Si la demande exige autorisation de sécurité de niveau très secret, continuez; si non, passez à l'étape 34. 28. Dans le cas des autorisations de sécurité de niveau très secret, le spécialiste du filtrage de sécurité du personnel déclenchera une évaluation de la sécurité par le SCRS. 29. Le spécialiste du filtrage de sécurité du personnel analyse les résultats de l'évaluation de la sécurité par le SCRS. 30. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 34. 31. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 34. 32. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). 33. Si aucun traitement supplémentaire n'est requis, passez à l'étape 50. 34. Si la demande exige une autorisation de sécurité du SIGNIT de niveau très secret, continuez; si non, passez à l'étape 39. 35. Dans le cas des autorisations de sécurité du SIGNIT de niveau très secret, le spécialiste du filtrage de sécurité du personnel déclenchera une vérification de la solvabilité supplémentaire. 36. Le spécialiste du filtrage de sécurité du personnel déclenchera ensuite une entrevue de l'URES avec le sujet. 37. Le processus de l'URES est déclenché (22 FT PSC FSP URES). 38. Si aucun traitement supplémentaire n'est requis, passez à l'étape 50. 39. Si une autorisation de sécurité de fiabilité approfondie de niveau très secret est requise, continuez; sinon passez à l'étape 48. 40. Dans le cas des autorisations de sécurité de fiabilité approfondie de niveau très secret, le spécialiste du filtrage de sécurité du personnel déclenchera un questionnaire ou une entrevue sur la sécurité. 41. Le spécialiste du filtrage de sécurité du personnel effectuera une enquête de sources ouvertes.

	42. Le spécialiste du filtrage de sécurité du personnel demandera une évaluation de la sécurité par le SCRS. 43. Le spécialiste du filtrage de sécurité du personnel demandera à la personne de se soumettre à un test polygraphique. 44. Le spécialiste du filtrage de sécurité du personnel analyse les résultats du questionnaire ou de l'entrevue sur la sécurité, de l'enquête de sources ouvertes, de l'évaluation de la sécurité par le SCRS et du test polygraphique. 45. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 48. 46. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 48. 47. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). Passez à l'étape 50. 48. Le spécialiste du filtrage de sécurité du personnel effectue une vérification de l'exhaustivité de la demande de filtrage de sécurité du personnel. 49. Le spécialiste du filtrage de sécurité du personnel crée le certificat de sécurité et l'envoie à l'ASE des organisations. 50. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande d'attestation de sécurité de personnel • Résultats des différentes vérifications de la sécurité (vérifications de solvabilité, évaluation de la sécurité par le SCRS, etc.)
Extrants	• Attribution de la demande d'attestation de sécurité du personnel • Certificat de sécurité

1.1.13 FSP – mise à jour

Le processus administratif de mise à jour d'une demande de FSP comprend la présentation d'informations aux fins de renouvellement ou de simple mise à jour. Les demandes de renouvellement sont traitées comme de nouvelles demandes de FSP, alors que les demandes de mise à jour exigent l'examen et l'analyse des renseignements fournis pour s'assurer de leur exhaustivité. Selon la nature de la mise à jour, ce processus administratif pourrait exiger d'autres vérifications d'antécédents qui pourraient influer sur l'ASP qui a déjà été délivrée. Dans le cas des processus habituels de mise à jour, un nouveau profil de sécurité est délivré. Si les renseignements demandés ne sont pas fournis, la demande d'ASP est fermée pour non-conformité.

Identification du flux des travaux	**15 FT mise à jour d'une demande FSP PSC**
Unité(s) opérationnelle(s)	Spécialiste du filtrage du PSC

Objectif opérationnel	Mettre à jour une ASP existante de la DFSP.
Élément déclencheur	Demande de mise à jour d'une ASP
Description du flux des travaux	1. Début du processus 2. Le spécialiste du filtrage du PSC détermine le type de mise à jour qui est effectué. S'il s'agit d'une mise à jour de renseignements existants, passez à l'étape 4. 3. Si la mise à jour vise un renouvellement, déclenchez le processus de création d'une nouvelle demande de FSP (14 FT nouvelle demande de FSP PSC), car il faut appliquer les mêmes exigences et les mêmes mesures. Passez à l'étape 15. 4. Le spécialiste du filtrage du PSC vérifie si la demande contient tous les renseignements nécessaires. Si tous les renseignements ont été reçus, passez à l'étape 7. 5. Le spécialiste du filtrage du PSC détermine s'il est nécessaire de demander des renseignements supplémentaires auprès de l'ASE de l'organisation. S'il est nécessaire d'obtenir des renseignements supplémentaires, passez à l'étape 4. 6. S'il n'est pas nécessaire d'obtenir des renseignements supplémentaires, le spécialiste du filtrage du PSC fermera la demande et retournera toute documentation originale à l'ASE. 7. Le spécialiste du filtrage du PSC mettra en jour les renseignements sur l'individu, en se fondant sur les renseignements fournis. 8. Le spécialiste du filtrage du PSC vérifiera s'il y a eu un changement dans la situation personnelle de l'individu. S'il y a eu un changement dans les circonstances personnelles, passez à l'étape 10. 9. S'il n'y a pas de changements dans les circonstances personnelles, le spécialiste du filtrage du PSC en informe le SCRS. 10. Le spécialiste du filtrage du PSC fournira de nouveaux renseignements au SCRS et lui demandera d'effectuer une nouvelle évaluation de sécurité. 11. Le spécialiste du filtrage de sécurité du personnel analyse les résultats de l'évaluation de la sécurité effectuée par le SCRS. S'il n'y a pas de résultats négatifs, passez à l'étape 13. 12. Si l'évaluation de sécurité effectuée par le SCRS a donné des résultats négatifs, le processus de l'URES (FT URES FSP PSC) est déclenché. Passez à l'étape 15. 13. Le spécialiste du filtrage du PSC effectue une vérification de l'exhaustivité de la demande. 14. Le spécialiste du filtrage du PSC crée un certificat de profil et l'envoie à l'ASE de l'organisation. 15. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande d'attestation de sécurité de personnel • Résultats de la vérification de sécurité effectuée par le SCRS
Extrants	• Certificat de sécurité

1.1.14 Filtrage de sécurité du personnel – Mise à niveau

Le processus opérationnel de mise à niveau de filtrage de sécurité du personnel comporte la mise à niveau d'une attestation de sécurité de personnel d'un niveau à un autre. La demande reçue est évaluée afin de déterminer si les vérifications de l'attestation de sécurité antérieures doivent être refaites. Après quoi, il est déterminé si la mise à niveau doit se poursuivre ou non. Si la mise à niveau doit se poursuivre, les vérifications de sécurité doivent être effectuées pour le niveau d'attestation voulu. S'il y a des résultats négatifs à tout moment durant le processus de mise à niveau de sécurité du personnel, le processus opérationnel de l'URES serait déclenché pour une dissipation des doutes. Si la mise à niveau de sécurité du personnel est réussie, une nouvelle attestation de sécurité sera attribuée et un certificat de sécurité fourni à l'organisation.

Identification du flux des travaux	**16 FT mise à jour d'une demande de FSP PSC**
Unité(s) opérationnelle(s)	• Spécialiste du filtrage du PSC
Objectif opérationnel	• Traitement d'une mise à niveau des demandes d'attestation de sécurité du personnel existantes.
Élément déclencheur	• Exigence de mise à niveau d'attestation de sécurité du personnel
Description du flux des travaux	1. Début du processus 2. Si la demande concerne une mise à niveau de la cote de fiabilité approfondie, continuez; sinon, passez à l'étape 16. 3. Le spécialiste du filtrage de sécurité du personnel évaluera la demande pour déterminer si les vérifications de la fiabilité/sécurité doivent être refaites. 4. S'il n'est pas nécessaire de refaire les vérifications de la fiabilité/sécurité, passez à l'étape 8. 5. Le spécialiste du filtrage de sécurité du personnel analyse les résultats des vérifications de la fiabilité/sécurité. S'il n'y a pas de résultats négatifs, passez à l'étape 7. 6. S'il y a des résultats négatifs, déclenchez le processus de l'URES (22 FT PSC FSP URES). 7. Si aucun traitement supplémentaire n'est requis, passez à l'étape 66. 8. Si un traitement supplémentaire est requis, le spécialiste du filtrage de sécurité du personnel déclenchera les vérifications de sécurité suivantes, vérification des documents sur le respect de la loi. 9. Le spécialiste du filtrage de sécurité du personnel demandera que la personne remplisse un questionnaire sur la sécurité ou passe une entrevue sur la sécurité. 10. Le spécialiste du filtrage de sécurité du personnel effectuera une enquête de sources ouvertes de la personne.

	11. Le spécialiste du filtrage de sécurité du personnel analyse les résultats de la vérification des documents sur le respect de la loi, du questionnaire/entrevue sur la sécurité et de l'enquête de sources ouvertes. 12. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 15. 13. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 15. 14. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). 15. Si aucun traitement supplémentaire n'est requis, passez à l'étape 64. 16. Si la demande concerne une mise à niveau d'autorisation de sécurité de niveau secret et d'accès aux sites, continuez; sinon, passez à l'étape 28. 17. Le spécialiste du filtrage de sécurité du personnel évaluera la demande pour déterminer si les vérifications de sécurité de niveau secret doivent être refaites. 18. S'il n'est pas nécessaire de refaire les vérifications de sécurité de niveau secret, passez à l'étape 22. 19. Le spécialiste du filtrage de sécurité du personnel analyse les résultats des vérifications de sécurité de niveau secret. S'il n'y a pas de résultats négatifs, passez à l'étape 21. 20. S'il y a des résultats négatifs, déclenchez le processus de l'URES (22 FT PSC FSP URES). 21. Si aucun traitement supplémentaire n'est requis, passez à l'étape 66. 22. Dans le cas des autorisations de sécurité de niveau secret et d'accès aux sites, le spécialiste du filtrage de sécurité du personnel déclenchera une évaluation de la sécurité par le SCRS. 23. Le spécialiste du filtrage de sécurité du personnel analyse les résultats de l'évaluation de la sécurité par le SCRS. 24. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 27. 25. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 27. 26. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). 27. Si aucun traitement supplémentaire n'est requis, passez à l'étape 64. 28. Si la demande concerne une mise à niveau d'autorisation de sécurité de niveau très secret, continuez; sinon, passez à l'étape 40. 29. Le spécialiste du filtrage de sécurité du personnel évaluera la demande pour déterminer si les vérifications de sécurité de niveau très secret doivent être refaites. 30. S'il n'est pas nécessaire de refaire les vérifications de sécurité de niveau très secret, passez à l'étape 34. 31. Le spécialiste du filtrage de sécurité du personnel analyse les résultats des vérifications de sécurité de niveau très secret. S'il n'y a pas de résultats négatifs, passez à l'étape 33. 32. S'il y a des résultats négatifs, déclenchez le processus de l'URES (22 FT PSC FSP URES). 33. Si aucun traitement supplémentaire n'est requis, passez à l'étape 66. 34. Dans le cas des autorisations de sécurité de niveau très secret, le spécialiste du filtrage de sécurité du personnel déclenchera une évaluation de la sécurité par le SCRS.

	35. Le spécialiste du filtrage de sécurité du personnel analyse les résultats de l'évaluation de la sécurité par le SCRS. 36. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 39. 37. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 39. 38. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). 39. Si aucun traitement supplémentaire n'est requis, passez à l'étape 64. 40. Si la demande concerne une mise à niveau d'autorisation de sécurité du SIGNIT de niveau très secret, continuez; sinon, passez à l'étape 41. 41. Le spécialiste du filtrage de sécurité du personnel évaluera la demande pour déterminer si les vérifications de sécurité du SIGNIT de niveau très secret doivent être refaites. 42. S'il n'est pas nécessaire de refaire les vérifications de sécurité du SIGNIT de niveau très secret, passez à l'étape 46. 43. Le spécialiste du filtrage de sécurité du personnel analyse les résultats des vérifications de sécurité du SIGNIT de niveau très secret. S'il n'y a pas de résultats négatifs, passez à l'étape 45. 44. S'il y a des résultats négatifs, déclenchez le processus de l'URES (22 FT PSC FSP URES). 45. Si aucun traitement supplémentaire n'est requis, passez à l'étape 66. 46. Dans le cas des autorisations de sécurité du SIGNIT de niveau très secret, le spécialiste du filtrage de sécurité du personnel déclenchera une vérification de la solvabilité supplémentaire. 47. Le spécialiste du filtrage de sécurité du personnel déclenchera ensuite une entrevue de l'URES avec le sujet. 48. Le processus de l'URES est déclenché (22 FT PSC FSP URES). 49. Si aucun traitement supplémentaire n'est requis, passez à l'étape 64. 50. La demande concerne la mise à niveau d'une autorisation de sécurité de fiabilité approfondie de niveau très secret. 51. Le spécialiste du filtrage de sécurité du personnel évaluera la demande pour déterminer si les vérifications de sécurité de niveau très secret doivent être refaites. 52. S'il n'est pas nécessaire de refaire les vérifications de sécurité de niveau très secret, passez à l'étape 56. 53. Le spécialiste du filtrage de sécurité du personnel analyse les résultats des vérifications de sécurité de niveau très secret. S'il n'y a pas de résultats négatifs, passez à l'étape 55. 54. S'il y a des résultats négatifs, déclenchez le processus de l'URES (22 FT PSC FSP URES). 55. Si aucun traitement supplémentaire n'est requis, passez à l'étape 66. 56. Dans le cas des autorisations de sécurité de fiabilité approfondie de niveau très secret, le spécialiste du filtrage de sécurité du personnel déclenchera un questionnaire ou une entrevue sur la sécurité. 57. Le spécialiste du filtrage de sécurité du personnel effectuera une enquête de sources ouvertes. 58. Le spécialiste du filtrage de sécurité du personnel demandera une évaluation de la sécurité par le SCRS. 59. Le spécialiste du filtrage de sécurité du personnel demandera à la personne de se soumettre à un test polygraphique. 60. Le spécialiste du filtrage de sécurité du personnel analyse les résultats du questionnaire ou de l'entrevue sur la sécurité, de l'enquête de sources ouvertes, de l'évaluation de la sécurité par le SCRS et du test polygraphique.

	61. Le spécialiste du filtrage de sécurité du personnel détermine s'il y a des résultats négatifs qui pourraient avoir une incidence sur l'attribution de l'attestation. S'il n'y a pas de résultats négatifs, passez à l'étape 64. 62. Le spécialiste du filtrage de sécurité du personnel détermine s'il doit appliquer la matrice du risque. Si la matrice doit être appliquée, passez à l'étape 64. 63. Si la matrice n'est pas applicable, déclenchez le processus de l'URES (22 FT PSC FSP URES). Passez à l'étape 66. 64. Le spécialiste du filtrage de sécurité du personnel effectue une vérification de l'exhaustivité de la demande de filtrage de sécurité du personnel. 65. Le spécialiste du filtrage de sécurité du personnel crée le certificat de sécurité et l'envoie à l'ASE des organisations. 66. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande d'attestation de sécurité de personnel • Résultats des différentes vérifications de la sécurité (vérifications de solvabilité, évaluation de la sécurité par le SCRS, etc.)
Extrants	• Attribution de la demande d'attestation de sécurité du personnel • Certificat de sécurité

1.1.15 Filtrage de sécurité du personnel – Transfert

Le processus opérationnel de transfert d'attestation de sécurité du personnel comprend le transfert d'une attestation de sécurité de personnel du PSC d'une organisation externe au PSC ou du PSC vers un autre ministère. Dans les deux cas, la validité de la demande de sécurité du personnel actuelle est vérifiée ainsi que si un renouvellement est requis avant le transfert. Lorsque l'attestation de sécurité actuelle n'est plus valide, la demande est fermée et on demande à l'organisation de soumettre une nouvelle demande. Les attestations de sécurité qui exigent un renouvellement sont simplement transférées à l'autre ministère destinataire avec une note au dossier.

Dans le cas du transfert d'attestation de sécurité du personnel au PSC, lorsque la cote demandée est supérieure au niveau d'attestation de sécurité actuel, on demande à l'organisation de soumettre une demande de mise à niveau d'attestation de sécurité et le transfert a lieu à ce niveau. L'attestation de sécurité transférée est ensuite évaluée afin de déterminer si des vérifications de sécurité doivent être refaites. Si les vérifications de sécurité donnent des résultats négatifs, le processus opérationnel de l'URES est évoqué pour une dissipation des doutes. Autrement, un nouveau certificat d'attestation de sécurité est attribué et fourni à l'organisation.

Identification du flux des travaux	**17 FT transfert d'une demande de FSP PSC**
Unité(s) opérationnelle(s)	• Spécialiste du filtrage du PSC

Objectif opérationnel	• Traiter le transfert d'une demande de filtrage de sécurité du personnel existante
Élément déclencheur	• Exigence de transfert de filtrage de sécurité du personnel.
Description du flux des travaux	1. Début du processus 2. Si l'attestation est demandée par un autre ministère en vue d'un transfert de SPAC, continuer; si la demande de transfert provient de SPAC, passez à l'étape 9. 3. Vérifiez si l'attestation existante est toujours active. 4. Si elle n'est pas valide, continuez; autrement, passez à l'étape 7. 5. Avisez l'autre ministère de l'invalidité de l'attestation et de l'impossibilité de transférer le dossier. 6. Fermez la demande, passez à l'étape 23. 7. S'il n'est pas nécessaire de renouveler l'attestation, continuez; autrement, passez à l'étape 9. 8. Joignez une note au dossier à l'autre ministère indiquant qu'un renouvellement est requis. 9. Envoyez une copie de l'attestation à l'autre ministère demandeur. 10. Avisez le SCRS du transfert de la demande, passez à l'étape 23. 11. Si l'autre ministère déclare que l'attestation n'est pas valide, continuez; autrement, passez à l'étape 14. 12. Fermez la demande de transfert. 13. Avisez l'ASE du besoin de soumettre une nouvelle demande puisque la demande de transfert ne peut pas être complétée. Passez à l'étape 23. 14. Si l'attestation ou la cote est gardée à un niveau inférieur à celui demandé, continuez; autrement, passez à l'étape 17. 15. Informez l'ASE qu'une demande de mise à niveau est requise pour que le niveau d'attestation demandé soit attribué. 16. Continuez le transfert au niveau de l'attestation ou de la cote du demandeur. 17. Évaluez la demande pour déterminer si les vérifications de sécurité doivent être refaites. 18. Si les vérifications de sécurité doivent être refaites, continuez; autrement, passez à l'étape 21. 19. Si les vérifications de sécurité effectuées de nouveau donnent des résultats négatifs, continuez; autrement, passez à l'étape 21. 20. Déclenchez le processus de l'URES (FT FSP URES PSC). 21. Vérifiez l'exhaustivité de la demande. 22. Créez un certificat d'enquête de sécurité en réponse à la demande et envoyez-le à l'ASE. 23. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande de transfert d'attestation de sécurité de personnel
Extrants	• Transfert de l'attestation ou de la cote de sécurité complétée

1.1.16 Filtrage de sécurité du personnel – duplication

Un processus administratif de duplication d'une attestation de sécurité du personnel (ASP) est suivi lorsque l'attestation vise une personne qui est employée par plusieurs organisations inscrites. Les attestations de sécurité sont validées, la demande est fermée et l'organisation est invitée à soumettre une nouvelle demande. L'ASP qui sera dupliquée est ensuite examinée pour déterminer si des vérifications de sécurité effectuées auparavant doivent être effectuées de nouveau. Si les vérifications de sécurité donnent des résultats négatifs, le processus de l'URES est déclenché pour dissiper tout doute qui pourrait subsister. Si aucun résultat négatif n'est constaté, un nouveau certificat d'enquête de sécurité et profil de sécurité est accordé et délivré à l'organisation.

Identification du flux des travaux	**18 FT duplication d'une demande de FSP PSC**
Unité(s) opérationnelle(s)	• Spécialiste du filtrage du PSC
Objectif opérationnel	• Traiter une demande de duplication d'une demande de FSP existante
Élément déclencheur	• Demande de duplication d'une demande de FSP
Description du flux des travaux	1. Début du processus 2. S'il n'existe aucune ASP valable au niveau demandé, continuez; sinon passe à l'étape 5. 3. Fermez la demande. 4. Informez l'agent de sécurité d'entreprise (ASE) du besoin de soumettre une nouvelle demande de FSP parce qu'il n'est pas possible de dupliquer le FSP au niveau demandé. Passez à l'étape 11. 5. Évaluez la demande précédente pour déterminer si d'autres vérifications de sécurité doivent être effectuées de nouveau. 6. Si des vérifications de sécurité doivent être effectuées de nouveau, continuez; si non, passez à l'étape 9. 7. Si les vérifications de sécurité qui sont effectuées de nouveau donnent des résultats négatifs, continuez; si non, passez à l'étape 9. 8. Déclenchez le processus de l'URES (22 FT FSP URES PSC). 9. Vérifiez l'exhaustivité de la demande. 10. Créez un certificat d'enquête de sécurité en réponse à la demande et envoyez-le à l'ASE. 11. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande d'ASP (duplication)

Extrants	• Certificat de sécurité

1.1.17 FSP – réactivation

Le processus administratif de réactivation d'une ASP vise à vérifier le temps écoulé depuis la résiliation d'une ASP et à déterminer s'il faut effectuer de nouveau les vérifications de sécurité. Si les vérifications de sécurité donnent des résultats négatifs, le processus de l'URES est déclenché pour dissiper tout doute qui pourrait subsister. Si aucun résultat négatif n'est constaté, l'ASP résiliée est dupliquée et réactivée. Une nouveau certificat d'enquête de sécurité et profil de sécurité est accordé et fourni à l'organisation.

Identification du flux des travaux	**19 FT réactivation d'une demande de FSP PSC**
Unité(s) opérationnelle(s)	• Spécialiste du filtrage du PSC
Objectif opérationnel	• Traiter une demande de réactivation d'une demande de FSP existante
Élément déclencheur	• Demande faite par une organisation de réactiver une demande de FSP.
Description du flux des travaux	1. Début du processus 2. Si l'ASP visée par la demande de réactivation est résiliée depuis plus de 2 ans, continuez; si non passez à l'étape 5. 3. Fermez la demande de réactivation. 4. Informez l'ASE du besoin de soumettre une nouvelle demande de FSP. Passez à l'étape 14. 5. Si l'ASP visée par la demande de réactivation est résiliée depuis 1 à 2 ans, continuez; si non passez à l'étape 9. 6. Effectuez de nouveau les vérifications de sécurité nécessaires. 7. Si les vérifications de sécurité effectuées de nouveau donnent des résultats négatifs, continuez; si non passez à l'étape 11. 8. Déclenchez le processus de l'URES (22 FT FSP URES PSC). 9. Si l'ASP visée par la demande de réactivation n'a pas encore été résiliée, continuez; si elle est résiliée depuis moins de 1 an, passez à l'étape 11. 10. Aucune demande de résiliation n'avait été reçue et l'ASP initiale est toujours active. 11. Dupliquez la demande d'ASP.

	12. Vérifiez l'exhaustivité de la demande. 13. Créez un certificat d'enquête de sécurité en réponse à la demande et envoyez-le à l'ASE. 14. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande d'ASP (réactivation)
Extrants	• Certificat de sécurité

1.1.18 FSP – résiliation

Le processus administratif de résiliation d'une ASP vise à s'assurer que la demande de résiliation contient tous les renseignements nécessaires; si non, la demande est fermée. S'il y a toute demande en attente auprès du SCRS, le SCRS en est informé et la résiliation de l'ASP est effectuée.

Identification du flux des travaux	**20 FT résiliation d'une demande de FSP PSC**
Unité(s) opérationnelle(s)	• Agent de sécurité de l'organisation • Spécialiste du filtrage de sécurité du personnel
Objectif opérationnel	• Résilier une ASP
Élément déclencheur	• Demande de résiliation d'une demande de FSP
Description du flux des travaux	1. Début du processus 2. L'ASE soumet une demande d'annulation d'une demande de FSP. Si la demande est soumise par l'entremise de Services en direct de sécurité industrielle (SEDSI), passez à l'étape 6. 3. Si l'ASE soumet une demande manuelle de résiliation d'une demande de FSP, le spécialiste du filtrage examine les renseignements fournis et vérifie si l'ASE a signé la demande. Si la demande ne pose aucun problème, passez à l'étape 7. 4. Si l'ASE n'a pas signé la demande de résiliation, le spécialiste du filtrage demande qu'il la signe. 5. Si le spécialiste du filtrage ne reçoit pas l'information, il ferme la demande. 6. Si l'ASE soumet une demande des SEDSI pour résilier une demande de FSP, la demande est comparée avec l'identification personnelle existante.

	7. Le spécialiste du filtrage vérifie s'il existe une demande de FSP en attente qui contient la même identification personnelle (pour la même organisation) auprès des SCRS. S'il n'y a pas de demande en suspens auprès des SCRS, passez à l'étape 9. 8. Si une demande de FSP pour la même organisation est toujours en suspens auprès des SCRS, le spécialiste du filtrage informera les SCRS de la demande de résiliation. 9. Le spécialiste du filtrage résilie la demande de FSP. 10. L'employé visé par le FSP est « rayé de l'effectif ». 11. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande de résiliation
Extrants	• Résiliation d'une ASP

1.1.19 FSP - Demandes de l'OTAN

Le processus d'ASP de l'OTAN vise à s'assurer de la réception de tous les renseignements nécessaires pour un certificat d'enquête de sécurité et profil de sécurité de l'OTAN visant une ASP pour l'échange de renseignements ou de biens avec les pays partenaires de l'OTAN. Si la personne répond aux critères et l'ASE a fourni les renseignements nécessaires à la Direction de la sécurité industrielle internationale (DSII), la demande de l'OTAN sera délivrée.

Identification du flux des travaux	**21 FT demandes OTAN PSC**
Unité(s) opérationnelle(s)	• Agent de sécurité de l'organisation • Partenaire de l'OTAN • Spécialiste du filtrage de sécurité du personnel
Objectif opérationnel	• Délivrer un certificat d'enquête de sécurité et profil de sécurité de l'OTAN pour une ASP
Élément déclencheur	• Demande d'attestation de l'OTAN
Description du flux des travaux	1. Début du processus 2. L'ASE soumet une demande d'attestation de l'OTAN. 3. La Division de filtrage de la sécurité du personnel soumet une demande de l'OTAN. 4. Le spécialiste du filtrage vérifie s'il existe une autorisation existante et valide pour l'individu (y compris une demande DC en attente de l'OTAN).

	5. S'il n'y a aucune autorisation valable, le spécialiste du filtrage soumet une demande d'ASP. 6. Le spécialiste du filtrage détermine le type/niveau d'attestation de sécurité requis et suivra le processus de la DFSP. 7. S'il y a une autorisation valide, le spécialiste du filtrage soumettra la demande de l'OTAN au flux de travail en attente de l'OTAN pour traitement par la DSII. 8. L'analyste de la DSII vérifiera d'abord si une attestation de sécurité nationale a été accordée. Si une attestation n'a pas été accordée, retournez à l'étape 5. 9. Si une attestation a été accordée, l'analyste de la DSII vérifiera si l'individu est un citoyen canadien. 10. Si l'individu est un citoyen canadien, l'analyste de la DSII déterminera si l'attestation de sécurité d'installation de l'OTAN respecte ou dépasse le niveau exigé. 11. Si l'individu n'est pas citoyen canadien, l'analyste de la DSII vérifiera si l'individu est un ressortissant de l'OTAN. 12. Si l'attestation de sécurité d'installation de l'OTAN atteint ou dépasse le niveau exigé et que l'individu est un ressortissant de l'OTAN qui réside au Canada depuis plus de 5 ans, passez à l'étape 19. Si l'attestation de sécurité d'installation de l'OTAN ne respecte pas le niveau exigé, passez à l'étape 13. 13. L'analyste de la DSII suit le processus de préparation d'une fiche de renseignement pour une ASP. 14. Si l'individu est citoyen canadien et un non-ressortissant de l'OTAN, l'analyste de la DSII déterminera si l'individu aura besoin d'une évaluation de sécurité du Bureau de sécurité de l'OTAN. Si non, passez à l'étape 17. 15. Si l'individu n'a pas besoin d'une une évaluation de sécurité du Bureau de sécurité de l'OTAN, l'analyste de la DSII vérifiera si les sections 42/42/44 indiquent que le non-ressortissant de l'OTAN a reçu une approbation de l'administration désignée en matière de sécurité. Si l'approbation n'est pas valide, passez à l'étape 17. 16. Si l'approbation est valide, l'analyste de la DSII suivra le processus de préparation d'une lettre de l'OTAN. 17. L'analyste de la DSII informera l'organisation des résultats de l'évaluation. 18. L'analyste de la DSII enverra un formulaire de profil à l'ASE pour qu'il le signe. 19. L'ASE doit retourner le formulaire signé à la DSII dans un délai de 10 jours ouvrables. 20. Si la DSII ne reçoit pas le formulaire dans ce délai, l'analyste de la DSII demandera à l'ASE de signer le formulaire. Si la DSII n'a pas reçu le formulaire de profil, passez à l'étape 26. 21. La DSII reçoit le formulaire de profil dans un délai de 10 jours ouvrables. 22. L'analyste de la DSII examine le formulaire de profil dûment signé. 23. L'analyste de la DSII fera correspondre la date d'expiration de l'OTAN avec la date d'expiration de l'attestation de sécurité nationale. 24. L'analyste de la DSII déterminera si la demande de l'OTAN est accordée ou refusée. 25. Si la DSII ne reçoit pas le formulaire de profil signé pour la demande de l'OTAN ou que l'analyste de la DSII refuse la demande, la demande de l'OTAN est fermée. 26. Si la DSII reçoit toute l'information requise pour la demande de l'OTAN, l'analyste de la DSII fournit les renseignements au partenaire étranger, à l'ASE et à l'individu. 27. Retournez au processus de demandes de FSP pour terminer (13 FT demande de FSP PSC).
Intrants	• Demande de l'OTAN

Extrants	• Certificat d'enquête de sécurité et profil de sécurité de l'OTAN pour une ASP

1.1.20 Filtrage de sécurité du personnel – Enquêtes

Le processus opérationnel des enquêtes du filtrage de sécurité du personnel vise à obtenir des renseignements supplémentaires sur le candidat. Une entrevue doit être réalisée pour évaluer l'admissibilité d'une personne à une attestation de sécurité. Cette entrevue porte sur les éléments suivants : le caractère de la personne, sa situation financière, la durée de ses séjours à l'étranger, ses croyances et ses relations personnelles. Le processus d'entrevue comprend un examen des résultats des vérifications de sécurité, comme des enquêtes relatives à l'existence d'un casier judiciaire, des vérifications de la fiabilité et des vérifications de la loyauté. Une entrevue peut être rendue nécessaire à la suite d'une inspection ou d'une enquête dans l'organisation s'il est survenu un incident lié à la sécurité. De même, la tenue d'une inspection ou d'une enquête dans l'organisation peut être déclenchée à la suite d'une entrevue avec un sujet.

Une entrevue avec le sujet doit être réalisée afin de déterminer la nature des circonstances ou de l'activité ayant causé un problème de sécurité au cours de l'enquête. Elle permet également à la personne concernée de fournir des renseignements précis pour répondre à ces préoccupations. Les entrevues individuelles sont obligatoires en vue d'obtenir les attestations de sécurité au niveau Top Secret SIGINT. Les responsables du PSC enverront une lettre recommandée à la personne concernée pour lui communiquer les résultats.

Identification du flux des travaux	**22 Processus du flux des travaux du PSC de l'URES**
Unité(s) opérationnelle(s)	• Division des inspections et des enquêtes • Spécialiste du filtrage de sécurité du personnel • Équipe de l'Unité responsable des enquêtes de sécurité (URES) • Directeur de la Direction de la sécurité industrielle canadienne (DSIC) • Équipe juridique de SPAC • Sous-ministre de SPAC
Objectif opérationnel	• Enquêter et déterminer l'admissibilité d'une attestation de sécurité pour le personnel.
Élément déclencheur	• Demande de filtrage de sécurité du personnel transmise à l'URES pour une enquête plus approfondie.

Description du flux des travaux	1. Début du processus. 2. La Division des inspections et des enquêtes présente une demande ou transmet des renseignements à l'URES (10 Inspection du flux des travaux du PSC ou 12 Inspection du flux des travaux du PSC). 3. La Division de filtrage de la sécurité du personnel (DFSP) reçoit une demande exigeant une enquête de l'URES. 4. La DFSP présente une demande ou transmet des renseignements à l'URES. 5. L'agent de liaison de l'URES vérifie si le dossier est complet et confirme les vérifications effectuées. 6. Si le dossier est incomplet, passez à l'étape 4. 7. Si le dossier est complet et si les vérifications ont été effectuées, une évaluation du SCRS doit être réalisée au besoin. 8. L'agent de liaison de l'URES transmet le dossier au chef de l'URES pour qu'il procède au tri. 9. Le chef de l'URES détermine si le filtrage de sécurité du personnel doit être suspendu. 10. Le chef de l'URES établit si le filtrage de sécurité du personnel doit être suspendu en se fondant sur le type de demande d'attestation de sécurité indiqué dans le dossier. 11. Si la demande d'attestation de sécurité se situe au niveau classifié, le dossier sera transmis au sous-ministre pour obtenir l'approbation de la suspension. 12. Si la demande d'attestation de sécurité se situe au niveau de la fiabilité, le dossier sera transmis au directeur de la DSIC pour obtenir l'approbation de la suspension. 13. Si le chef de l'URES détermine qu'il n'y a pas lieu de suspendre la demande, le chef établira si une enquête de l'URES est requise. Si aucune enquête n'est requise, passez à l'étape 28. 14. Si une enquête de l'URES est requise, le chef de l'URES affecte le dossier à un agent de l'URES aux fins d'exécution. 15. L'agent de l'URES se prépare à tenir une entrevue visant à dissiper les doutes avec la personne visée. 16. L'agent de l'URES mène une entrevue visant à dissiper les doutes avec la personne visée. 17. Après l'entrevue, l'agent de l'URES procède à la vérification et à la validation des résultats de l'entrevue de dissipation des doutes. 18. L'agent de l'URES remplit un rapport et formule une recommandation concernant le dossier. 19. Si l'agent de l'URES recommande un refus du filtrage de la sécurité du personnel, il prépare une trousse de refus. 20. L'agent de l'URES doit déterminer si une entrevue de suivi est requise avec la personne visée. 21. Si une entrevue de suivi est requise, l'agent de l'URES fixera un rendez-vous à cet effet avec la personne. 22. Si une entrevue de suivi n'est pas requise, l'agent de l'URES transmettra un rapport avec sa recommandation au chef de l'URES pour que celui-ci l'examine. 23. Le chef de l'URES examine le rapport et la recommandation. 24. Le chef de l'URES détermine s'il y a lieu de tenir une entrevue de suivi avec la personne. Si une entrevue de suivi est requise, passez à l'étape 21. 25. Si une entrevue de suivi n'est pas requise, le chef de l'URES détermine s'il y a lieu d'apporter des modifications au rapport et à la recommandation proposée. 26. Si le chef de l'URES détermine que des modifications sont requises, l'agent de l'URES modifie le rapport et la recommandation en conséquence. Une fois les modifications apportées, passez à l'étape 22.

	27. Si le chef de l'URES détermine qu'aucune modification n'est requise, il attribue le dossier à l'agent de liaison de l'URES aux fins d'exécution en se fondant sur la recommandation indiquée dans le rapport. 28. Si la recommandation consiste à accepter la demande de filtrage de la sécurité du personnel, passez à l'étape 29. 29. L'agent de liaison de l'URES accorde la demande de filtrage de la sécurité du personnel. 30. L'agent de liaison de l'URES vérifie si d'autres étapes de traitement sont requises. Si aucune autre étape de traitement n'est requise, passez à l'étape 50. 31. Si l'agent de liaison de l'URES détermine que d'autres étapes de traitement sont requises, le dossier est transmis au flux de travail approprié aux fins d'exécution par la DFSP. 32. Si la recommandation consiste à fermer la demande de filtrage de la sécurité du personnel, passez à l'étape 33. 33. L'agent de liaison de l'URES crée la lettre de fermeture et la transmet à l'ASE. Une fois la lettre transmise, passez à l'étape 50. 34. Si la recommandation consiste à mettre fin à la demande de filtrage de la sécurité du personnel, passez à l'étape 35. 35. L'agent de liaison de l'URES informe l'ASE qu'une demande de cessation du filtrage de la sécurité du personnel doit être transmise à la DFSP aux fins d'exécution. Une fois que l'ASE a été informé, passez à l'étape 50. 36. Si la recommandation consiste à refuser ou à révoquer la demande de filtrage de la sécurité du personnel, passez à l'étape 37. 37. Le rapport et la lettre de refus sont examinés par l'équipe juridique. 38. Si l'équipe juridique détermine qu'aucune modification du rapport ou de la lettre de refus n'est requise, passez à l'étape 40. 39. Le chef de l'URES doit corriger le rapport et la lettre de refus proposés par l'équipe juridique. Une fois terminé, passez à l'étape 37. 40. Le rapport et la lettre de refus seront examinés de nouveau par l'équipe juridique aux fins d'approbation finale. 41. Si le type de demande d'attestation de sécurité du dossier se situe au niveau de la fiabilité, le directeur de la DSIC doit examiner le rapport et la lettre de refus. Si aucune modification n'est proposée par le directeur de la DSIC, passez à l'étape 44. 42. Si le directeur de la DSIC détermine que des modifications doivent être apportées au rapport ou à la lettre de refus, passez à l'étape 43. 43. Le chef de l'URES doit modifier le rapport et la lettre de refus conformément aux modifications proposées par le directeur de la DSIC. Une fois terminé, passez à l'étape 41. 44. Le directeur de la DSIC approuvera ou refusera la recommandation. Si le directeur de la DSIC approuve le refus, passez à l'étape 49. Si le directeur de la DSIC n'approuve pas le refus, la prochaine étape du processus est en cours d'élaboration et n'est pas encore connue pour le moment. 45. Si le type de demande d'attestation de sécurité vise le niveau classifié, le sous-ministre doit examiner le rapport et la lettre de refus. 46. Si le sous-ministre détermine que des modifications doivent être apportées au rapport ou à la lettre de refus, passez à l'étape 47.

	47. Le dossier est retourné au chef de l'URES pour corriger le rapport et la lettre de refus conformément aux modifications proposées par le sous-ministre. 48. Si le sous-ministre approuve le rapport et la lettre de refus, passez à l'étape 49. Si le sous-ministre n'approuve pas le rapport et la lettre de refus à cette étape du processus, la prochaine étape est en cours d'élaboration et n'est pas encore connue pour le moment. 49. L'agent de liaison de l'URES transmettra un avis à l'ASE, à la personne visée et au SCRS pour les informer de la décision. 50. Fin du processus.
Intrants	• Admissibilité des attestations de sécurité pour le personnel
Extrants	• Délivrance ou révocation des attestations de sécurité pour le personnel

1.1.21 Centre d'appels

Le centre d'appels du Programme de sécurité industrielle (PSI) répond aux demandes des divers clients sur le Programme de sécurité des contrats (PSC) et le Programme des marchandises contrôlées (PMC). Dans la mesure du possible, le centre d'appels fournit la réponse. À défaut, la demande est évaluée puis confiée au secteur d'activité approprié du PSC ou du PMC, pour une réponse ou une action.

Identification du flux des travaux	**23 Flux des travaux du centre d'appels du PSC**
Entité(s)	• Contact externe (agent de sécurité des contrats, représentant désigné, etc.) • Analyste du centre d'appels • Analyste principale du centre d'appels • Secteur d'activité du PSI (PSC ou PMC)
Objectif opérationnel	• Description des activités du centre d'appels, de la réception de la demande à la réponse.
Élément déclencheur	• Requête d'un client auprès du Secteur de la sécurité industrielle (SSI).

Description du flux des travaux	1. Début du processus. 2. Un client ne faisant pas partie du PSI soumet une demande de renseignements au centre d'appels. Cette demande peut se faire sous la forme d'un appel téléphonique, d'un message vocal ou d'un courriel. 3. L'analyste du centre d'appels détermine si l'information peut être communiquée à la personne faisant la demande. Si tel est le cas, il continue à l'étape 4. Si l'information ne peut être communiquée, il en avise la personne et passe à l'étape 17. 4. L'analyste du centre d'appels examine la demande de renseignements afin de déterminer s'il s'agit d'une demande de niveau 1. Une demande de niveau 1 se caractérise par une réponse facile à obtenir à partir d'outils existants et pouvant être fournie immédiatement. Si la demande est de niveau 1, allez à l'étape 13. Dans le cas contraire, poursuivez à l'étape 5. 5. L'analyste du centre d'appels détermine si la demande est de niveau 2. Une demande de niveau 2 se caractérise par une réponse détaillée nécessitant un niveau d'interprétation ou de jugement. Si la demande est de niveau 2, allez à l'étape 7. Dans le cas contraire, allez à l'étape 6. 6. La demande est de niveau 3 si elle requiert une réponse du secteur d'activité compétent du PSI (PSC ou PMC). Passez à l'étape 8. 7. L'analyste du centre d'appels détermine si la demande de niveau 2 nécessite l'aide de l'analyste principal du centre d'appels. Si aucune aide n'est requise, passez à l'étape 13, sinon continuez à l'étape 8. 8. L'analyste principal du centre d'appels détermine si un triage de la demande est nécessaire. Si un triage n'est pas nécessaire, allez à l'étape 11, sinon poursuivez à l'étape 9. 9. L'analyste principal du centre d'appels évalue la demande de renseignements pour déterminer à quel secteur d'activité du PSI elle doit être transférée. 10. L'analyste principal du centre d'appels envoie la requête au secteur d'activité du PSI concerné afin d'obtenir une réponse. Continuez à l'étape 12. 11. L'analyste principal du centre d'appels et l'analyste du centre d'appels établissent conjointement une réponse à la demande de renseignements. Allez à l'étape 14. 12. Le secteur d'activité du PSI formule la réponse à la demande. Continuez à l'étape 14. Si le secteur d'activité du PSI fournit la réponse directement au client, allez à l'étape 16. 13. L'analyste du centre d'appels formule la réponse à la demande. 14. L'analyste du centre d'appels fournit au client la réponse à sa demande. 15. L'analyste du centre d'appels consigne l'appel dans le Système d'information sur la sécurité ministérielle et industrielle (SISMI) aux fins de suivi. 16. Le secteur d'activité du PSI fournit la réponse au client. 17. Le processus se termine.
Intrants	• Demande de renseignements d'un client.
Extrants	• Réponse à la demande de renseignements d'un client.

1.1.22 Visites du PSC

Le PSC traite les demandes de visite de site sécurisé nationale et internationale. En tant qu'administration désignée en matière de sécurité (ADS) au Canada, le PSC assure la protection de la sécurité nationale en veillant à que les exigences en matière de sécurité des contrats soient respectées, empêchant ainsi tout accès non autorisé aux renseignements et aux biens de nature délicate.

Identification du flux des travaux	**24 Flux des travaux – Visites du PSC**
Unités opérationnelles	• Responsables de la sécurité • Agents chargés des visites du PSC
Objectif opérationnel	• Traiter les demandes de visite de l'intérieur et de l'extérieur du Canada et s'assurer que les exigences en matière de sécurité soient maintenues.
Déclencheur	• L'industrie canadienne ou le gouvernement du Canada doivent parfois visiter d'autres sites canadiens, américains ou étrangers. Il en va de même pour les États-Unis ou les entités étrangères qui souhaitent visiter un site de l'industrie canadienne ou du gouvernement du Canada.
Description du flux des travaux	1. Début du processus 2. Le responsable de la sécurité soumet une demande de visite (DV) au PSC. Les DV peuvent servir à l'un des nombreux types de visite et sont généralement soumises de manière suivante : a. Les demandes de visite du Canada vers le Canada, du Canada vers les États-Unis et du Canada vers l'étranger sont reçues par courriel. b. Les demandes de visite des États-Unis vers le Canada sont reçues par l'intermédiaire du Defence Security Service (DSS) du Department of Defence des États-Unis, qui sont reçues par le MDN et transmises au PSC par courriel du directeur - Liaison avec l'étranger (DLE3) du MDN. c. Les demandes de visites de l'étranger vers le Canada sont reçues par le directeur – Liaison avec l'étranger (DLE3) du MDN et transmises au PSC par courriel. Elles peuvent aussi être reçues par un courriel direct de l'étranger au PSC. 3. L'agent chargé des visites du PSC examine la DV. 4. L'agent chargé des visites du PSC valide les exigences de sécurité de la visite. Cela se fait en examinant le contrat cité en référence, le niveau et l'état de l'attestation de l'organisation ainsi que les niveaux des cotes de sécurité individuelles tels que requis. Dans le cas de visites de l'étranger vers le Canada ou à partir du Canada, on demande que le pays valide les niveaux d'attestation de l'organisation et des personnes et en fournisse l'assurance.

	5. L'agent chargé des visites du PSC détermine si la DV est complète. Le cas échéant, allez à l'étape 9, 14, 15, 18 ou 19 selon le type de visite; autrement, continuez à l'étape 6. 6. L'agent chargé des visites du PSC détermine si la DV doit être rejetée ou non. S'il décide que la DV doit être rejetée, allez à l'étape 25; autrement, continuez à l'étape 7. 7. L'agent chargé des visites du PSC envoie une demande à l'agent de sécurité des DV pour obtenir les renseignements manquants. 8. Le responsable de la sécurité fournit les renseignements demandés. Allez à l'étape 3. 9. Le type de DV est une visite du Canada vers le Canada. 10. La visite du Canada vers le Canada est soit une visite de l'industrie sous-type soit une visite du MDN. S'il s'agit du MDN, allez à l'étape 13, autrement, continuez à l'étape 11. 11. L'agent chargé des visites du PSC demande l'accord du site hôte pour la visite. 12. L'agent chargé des visites du PSC reçoit la réponse du site hôte indiquant son accord. Allez à l'étape 24. 13. L'agent chargé des visites du PSC envoie la DV au MDN. Allez à l'étape 24. 14. Le MDN approuve la DV et avise le PSC. Allez à l'étape 24. 15. Le type de DV est une visite des États-Unis vers le Canada. Allez à l'étape 17. 16. Le type de DV est une visite de l'étranger vers le Canada. 17. L'agent chargé des visites du PSC demande l'accord du site hôte. 18. L'agent chargé des visites du PSC reçoit la réponse indiquant l'accord du site hôte. Allez à l'étape 24. 19. Le type de DV est une visite du Canada vers l'étranger. Allez à l'étape 21. 20. Le type de DV est une visite du Canada vers les États-Unis. 21. L'agent chargé des visites du PSC demande l'accord de l'ASM étranger. 22. L'agent chargé des visites du PSC reçoit l'accord de l'ASM étranger. 23. L'agent chargé des visites du PSC détermine si la DV doit être approuvée. Si la DV n'est pas approuvée, allez à l'étape 25, autrement, continuez à l'étape 24. 24. L'agent chargé des visites du PSC crée l'avis d'autorisation de la DV. Allez à l'étape 26. 25. L'agent chargé des visites du PSC crée l'avis de rejet de la DV. 26. L'agent chargé des visites du PSC envoie l'avis au responsable de la sécurité qui a soumis la DV et au site hôte de la visite. 27. Le processus prend fin.
Intrants	• Demande de visite • Clauses sur la sécurité des contrats • Accord du site hôte
Extrants	• Demande d'approbation ou de rejet de la visite • Avis d'autorisation ou de rejet

1.2 PROCESSUS DU PROGRAMME DES MARCHANDISES CONTRÔLÉES

1.2.1 Inscription au Programme des marchandises contrôlées - Nouveau

Identification du flux des travaux	25 Flux des travaux de l'inscription au PMC Nouveau
Unité(s) opérationnelle(s)	• Organisation qui s'inscrit (demandeur) • Commis de soutien du PMC • Agent d'information du soutien du PMC • Coordonnateur de l'inscription au PMC • Chef de l'inscription au PMC • Analyste de l'inscription au PMC • Gestionnaire des opérations du PMC • Gestion de cas et des pratiques exemplaires (GCPE) du PMC • Unité d'analyse et de recherches (UAR) du PMC • Gestion de programmes et Apprentissage (GPA) du PMC • Conformité au PMC
Objectif opérationnel	• Pour inscrire une nouvelle organisation au soutien en service (SES) du Programme des marchandises contrôlées (PMC).
Élément déclencheur	• L'organisation est tenue de s'inscrire auprès du SES du PMC parce qu'elle est en possession de marchandises contrôlées ou qu'elle a accès à de telles marchandises.
Description du flux des travaux	1. Début du processus. 2. Le demandeur remplit et soumet une demande d'inscription au PMC. 3. Le commis de soutien du PMC examine la demande d'inscription. 4. Le commis de soutien du PMC détermine si tous les renseignements requis ont été reçus. Si tous les renseignements ont été reçus, passez à l'étape 7. 5. S'il manque des renseignements, le commis de soutien du PMC invite le demandeur à lui fournir les renseignements manquants. 6. Le demandeur fournit les renseignements demandés, passez à l'étape 2. 7. Le commis de soutien du PMC effectue la saisie des données préliminaires. 8. L'agent d'information de soutien du PMC valide la demande. 9. L'agent d'information de soutien du PMC détermine si tous les renseignements requis ont été reçus. Si tous les renseignements ont été reçus, passez à l'étape 14.

	10. L'agent d'information de soutien du PMC détermine si la demande doit être rejetée parce qu'elle est incomplète. Si la demande est rejetée, passez à l'étape 13. 11. Si la demande n'est pas rejetée, l'agent d'information de soutien du PMC invite le demandeur à fournir les renseignements qui manquent. 12. Le demandeur fournit les renseignements manquants. Passez à l'étape 8. 13. Si la demande est rejetée à partir de l'étape 10, l'agent d'information de soutien du PMC avise le demandeur que sa demande a été rejetée. Passez à l'étape 48. 14. Si tous les renseignements ont été reçus, le commis de soutien du PMC complète la saisie des données de la demande. 15. L'agent d'information de soutien du PMC procède au contrôle de la qualité des données saisies. 16. L'agent d'information de soutien du PMC examine la demande d'évaluation de la sécurité du demandeur (DES) dans le cadre de la demande d'inscription. 17. L'agent d'information de soutien du PMC avise le demandeur que l'inscription au Programme est en cours de traitement. 18. L'agent d'information de soutien du PMC demande des vérifications de sécurité (empreintes digitales, vérification nominale du casier criminel, vérification de crédit, etc.) au besoin. 19. L'agent d'information de soutien du PMC informe Gestion de programmes et Apprentissage (DGPA) si le représentant désigné (RD) d'une organisation a besoin de formation. 20. Le processus de formation du PMC est déclenché. (Flux de travail de la formation du RD du PMC). 21. Le coordonnateur de l'inscription au PMC procède au tri et à l'attribution de la demande d'inscription à un analyste de l'inscription au PMC aux fins de traitement. 22. L'analyste de l'inscription au PMC vérifie si la demande et la demande d'évaluation de la sécurité sont complets. 23. L'analyste de l'inscription au PMC détermine si tous les renseignements requis ont été reçus. Si tous les renseignements requis ont été reçus, passez à l'étape 26. 24. L'analyste de l'inscription au PMC invite le demandeur à fournir les renseignements manquants. 25. Le demandeur fournit les renseignements manquants. Passez à l'étape 22. 26. L'analyste de l'inscription au PMC complète la saisie des données d'inscription. 27. L'analyste de l'inscription au PMC analyse la demande et la demande d'évaluation de la sécurité. 28. L'analyste de l'inscription au PMC détermine s'il est nécessaire de procéder à un renvoi à l'Unité d'analyse et de recherches (UAR). Si aucun renvoi n'est requis, passez à l'étape 30. 29. Si un renvoi à l'UAR du PMC est requis, le processus de l'UAR du PMC est déclenché. (Flux des travaux du renvoi pour motif valable du PMC). Passez à l'étape 32. 30. L'analyste de l'inscription au PMC détermine s'il y a lieu de procéder à un renvoi à Gestion de cas et pratiques exemplaires (GCPE) du PMC. S'il n'est pas nécessaire de procéder à un renvoi à GCPE du PMC, passez à l'étape 32. 31. S'il est nécessaire de procéder à un renvoi à GCPE du PMC, le processus de gestion de cas et pratiques exemplaires est déclenché (34 flux des travaux de la GCPE du PMC). Passez à l'étape 32. 32. L'analyste de l'inscription du PMC analyse tous les résultats des étapes précédentes et détermine si la demande d'inscription au PMC doit être approuvée, rejetée ou si le cas présente des risques élevés. Si la demande d'inscription au PMC est rejetée, passez à l'étape 35. Si la demande d'inscription au PMC est approuvée, passez à l'étape 38.

	33. Si la demande d'inscription au PMC est considérée à risque élevé, l'analyste de l'inscription au PMC crée une demande visant à communiquer le risque aux paliers supérieurs. 34. Le gestionnaire des opérations du PMC amorce le processus d'acheminement au palier hiérarchique approprié et prend la décision de rejeter ou d'approuver la demande d'inscription au PMC. Passez à l'étape 32. 35. Si la demande d'inscription au PMC est rejetée, l'analyste de l'inscription au PMC crée un rapport de rejet. 36. Le chef de l'inscription au PMC procède au contrôle de la qualité du rapport de rejet. 37. Si le contrôle de la qualité du rapport de rejet donne des résultats positifs, passez à l'étape 48. Si le contrôle de la qualité du rapport de rejet échoue, l'analyste de l'inscription au PMC doit lui apporter des modifications, passez à l'étape 35. 38. Si la demande d'inscription au PMC est approuvée, l'analyste de l'inscription au PMC crée un rapport d'approbation. 39. Le chef de l'inscription au PMC procède au contrôle de la qualité du rapport d'approbation. 40. Si le contrôle de la qualité du rapport d'approbation échoue, l'analyste de l'inscription au PMC doit lui apporter des modifications, passez à l'étape 38. 41. Si le contrôle de la qualité du rapport d'approbation donne des résultats positifs, le chef de l'inscription au PMC effectue la saisie de quelques données. 42. Le chef de l'inscription au PMC active les établissements de l'organisation à l'intérieur du système opérationnel du PMC. 43. Le chef de l'inscription au PMC approuve la demande d'évaluation de la sécurité de l'organisation et de la personne autorisée. 44. L'analyste de l'inscription au PMC met un point final à la saisie des données. 45. L'analyste de l'inscription au PMC crée une demande d'inspection, laquelle déclenche le flux de travail de l'inspection du PMC. 46. Le flux de travail de l'inspection du PMC est déclenché (30 Flux de travail des inspections du PMC). 47. L'analyste de l'inscription au PMC crée et envoie à l'organisation la trousse de correspondance sur l'inscription. 48. Fin du processus.
Intrants	• Demande d'inscription de l'organisation • Demandes d'évaluation de sécurité individuelles • Vérifications de sécurité
Extrants	• Approbation ou rejet de la demande d'inscription au PMC • Trousse d'inscription au PMC • Déclenchement de divers autres processus liés au PMC comme le processus de formation du PMC, le processus de l'UAR du PMC, etc.

1.2.2 Inscription au Programme des marchandises contrôlées - Modifications

Identification du flux des travaux	26 Flux des travaux des modifications à l'inscription au PMC
Unité(s) opérationnelle(s)	• Inscription de la personne autorisée (PA) ou du représentant désigné (RD) de l'organisation • Commis de soutien du PMC • Agent d'information du soutien du PMC • Coordonnateur de l'inscription au PMC • Unité d'analyse et de recherches (UAR) du PMC • Gestion de programmes et Apprentissage (GPA) du PMC • Conformité au PMC
Objectif opérationnel	• Appliquer les modifications aux renseignements concernant une organisation inscrite au PMC. Il peut s'agir de l'un des types de modifications suivants : o Demande de cessation de l'inscription de l'organisation o Modification aux renseignements du PMC o Présentation d'une évaluation de sécurité o Présentation d'une évaluation de l'entreprise o Présentation du consentement des ressortissants étrangers o Présentation des demandes d'exemption pour travailleurs temporaires ou visiteurs • Il existe cinq types de modifications : o Type 1 : il s'agit de modifications simples qui peuvent être transmises par courriel. Comprend des éléments tels que : ▪ Correction de coquilles ou de fautes d'orthographe ▪ Modification au consentement à mettre en ligne sur le site Web du PMC ▪ Enlever un représentant de l'entreprise **(sauf PA, propriétaire ou RD)** ▪ Enlever des RD **(L'installation doit avoir au moins un RD)** ▪ Ajouter un RD approuvé à une installation activée o Type 2 : qui exige une demande d'évaluation de sécurité. Comprend des éléments tels que : ▪ Nouveaux RD o Type 3 : qui exige une demande d'inscription. Comprend des éléments tels que : ▪ Changement d'adresse pour une installation existante ▪ Ajout d'installation(s) ▪ Enlèvement d'installation(s)

	▪ Changement d'une PA qui n'aura pas accès aux marchandises contrôlées – enlever une fois que les changements REG ont été approuvés ▪ Ajout ou changement dans les représentants d'entreprise ▪ Changement de raison sociale ▪ Changement de nom d'entreprise ▪ Changement de propriétaire (n'inclut pas les personnes qui doivent faire l'objet d'une évaluation de sécurité par le PMC) ▪ Regroupement(s) d'entreprises ○ Type 4 : qui exige à la fois une demande d'inscription et une demande d'évaluation de sécurité. Comprend des éléments tels que : ▪ Nouvelle personne canadienne autorisée qui aura accès aux marchandises contrôlées ▪ Nouveau(x) propriétaire(s) canadien(s) possédant au moins 20 % des actions donnant droit de vote ○ Type 5 : qui nécessite d'autres formulaires. Comprend des éléments tels que : ▪ Nouveau(x) propriétaire(s) étranger(s) possédant au moins 20 % des actions donnant droit de vote (nécessite le formulaire de consentement des ressortissants étrangers) ▪ Nouveau ressortissant étranger autorisé (nécessitant une demande pour travailleur étranger)
Élément déclencheur	• Présentation d'une demande de modification par une PA ou un RD pour les motifs suivants : ○ Demande de cessation de l'inscription de l'organisation ○ Modification aux renseignements du PMC ○ Présentation d'une évaluation de sécurité ○ Présentation d'une évaluation de l'entreprise ○ Présentation du consentement des ressortissants étrangers ○ Présentation des demandes d'exemption pour travailleurs temporaires ou visiteurs
Description du flux des travaux	1. Début du processus 2. Le demandeur présente une demande de modification au PMC. 3. Le commis de soutien du programme du PMC reçoit et examine la demande de modification. Si la demande de modification concerne des changements de numéro de téléphone, de numéro de télécopieur ou d'adresse électronique, passez à l'étape 3, sinon, passez à l'étape 4. 4. Le commis de soutien du PMC applique la modification. Passez à l'étape 28. 5. Si la demande de modification concerne l'exemption pour un travailleur temporaire, passez à l'étape 4, sinon, passez à l'étape 7. 6. Le processus d'exemption pour les travailleurs étrangers de l'UAR du PCM est déclenché (31 flux des travaux de l'exemption pour travailleur étranger du PMC). 7. Le coordonnateur de l'inscription du PMC reçoit la demande de modification, et passe en revue les renseignements qu'elle contient. Si les renseignements sont complets, passez à l'étape 9. 8. Si les renseignements de la demande de modification sont jugés incomplets par le coordonnateur de l'inscription, demandez au demandeur de fournir les renseignements manquants.

	9. Le demandeur fournit les renseignements demandés, passez à l'étape 1. 10. Si les renseignements relatifs à la demande de modification sont complets, le coordonnateur de l'inscription du PMC classera la modification. Le classement de la modification détermine les intrants et les mesures qui sont requis pour cette modification en particulier. 11. Si le coordonnateur de l'inscription du PMC détermine qu'il s'agit d'une modification à titre informatif seulement, passez à l'étape suivante, sinon, passez à l'étape 15. 12. Le coordonnateur de l'inscription du PMC appliquera la modification de l'information. 13. Si la modification de l'information ne déclenche pas de changement dans le niveau de risque, passez à l'étape 15. Sinon, la modification de l'information entraîne effectivement un changement dans le niveau de risque, et le coordonnateur de l'inscription du PMC en informe la Conformité du PMC. 14. Le processus d'inspection du PMC est déclenché (30 Flux de travail des inspections du PMC). 15. Si le coordonnateur de l'inscription du PMC détermine qu'il s'agit d'une demande de cessation de l'inscription de l'organisation. 16. Si la modification vise une cessation d'inscription, le coordonnateur de l'inscription du PMC prépare la lettre de cessation de l'inscription qui est envoyée à la PA ou au RD de l'organisation. 17. Le coordonnateur de l'inscription du PMC applique aussi la modification visant la cessation de l'inscription de l'entreprise, il met fin à l'inscription de cette dernière, et déclenche une inspection de fermeture par Conformité du PMC, passez à l'étape 14. 18. Si le coordonnateur de l'inscription du PMC détermine qu'une évaluation de sécurité est requise, continuez jusqu'à l'étape suivante, sinon, passez à l'étape 21. 19. Le coordonnateur de l'inscription du PMC effectue une évaluation de sécurité. 20. Le coordonnateur de l'inscription du PMC applique les renseignements résultant de l'évaluation de sécurité à l'organisation. 21. Une fois que le coordonnateur de l'inscription du PMC a effectué l'évaluation de sécurité, s'il n'est pas nécessaire de donner de la formation, passez à l'étape 23. 22. Si le coordonnateur de l'inscription du PMC détermine qu'il faut donner de la formation, il en avise GPA du PMC. Le processus de formation du PMC est déclenché (28 Flux des travaux de la conduite de la formation du RD du MC). 23. Si le coordonnateur de l'inscription du PMC détermine que la modification nécessite l'évaluation de l'entreprise, continuez jusqu'à l'étape suivante, sinon, passez à l'étape 25. 24. Le coordonnateur de l'inscription du PMC effectue une évaluation de l'entreprise. Si au cours de l'évaluation de l'entreprise le coordonnateur de l'inscription du PMC constate qu'il est nécessaire d'effectuer une évaluation de sécurité, passez à l'étape 18. 25. Le coordonnateur de l'inscription du PMC estime qu'il faut procéder à un renvoi pour motif valable à l'UAR. S'il n'est pas nécessaire de procéder à un renvoi pour motif valable, passez à l'étape 27. 26. Le processus de renvoi pour motif valable à l'UAR du PMC est déclenché (29 Flux des travaux de l'Unité d'analyse et de recherches [UAR] du PMC). Les résultats du « Renvoi pour motif valable » déclenchent à nouveau la nécessité d'effectuer une évaluation de l'entreprise, passez à l'étape 23.

	27. Le coordonnateur de l'inscription du PMC applique la modification relative à l'évaluation de l'entreprise. 28. Fin du processus.
Intrants	• Modification présentée
Extrants	• Modification traitée • Déclenchement de divers autres processus du PMC.

1.2.3 Inscription au Programme des marchandises contrôlées – Renouvellement

Identification du flux des travaux	27 Flux des travaux du renouvellement de l'inscription au PMC
Entité(s)	• Organisation demandant l'inscription (demandeur) • Commis de soutien du PMC • Agent d'information et de soutien du PMC • Coordonnateur de l'inscription du PMC • Directeur de l'inscription du PMC • Analyste de l'inscription du PMC • Gestionnaire des opérations du PMC • Gestion des cas et pratiques exemplaires (GCPE) du PMC • Unité d'analyse et de recherches (UAR) du PMC • Apprentissage et gestion du PMC • Conformité du PMC
Objectif opérationnel	• Renouveler l'inscription d'une organisation au Programme des marchandises contrôlées (PMC) du Secteur de la sécurité industrielle (SSI).
Élément déclencheur	• Une organisation doit renouveler son inscription au PMC du SSI, car elle est en possession de marchandises contrôlées ou a accès à de telles marchandises.
Description du flux des travaux	1. Début du processus. 2. Le commis de soutien du PMC dresse la liste des organisations dont l'inscription au PMC arrive à échéance et les informe des conditions de renouvellement. 3. Le demandeur remplit et soumet la demande d'inscription au PMC. 4. Le commis de soutien du PMC examine la demande d'inscription.

	5. Le commis de soutien du PMC vérifie que toute l'information exigée a été reçue. Si toutes les informations requises ont été reçues, allez à l'étape 7. 6. Si des informations sont manquantes, le commis de soutien du PMC les réclame au demandeur. 7. Le postulant fournit les informations demandées, allez à l'étape 3. 8. Le commis de soutien du PMC effectue la saisie des données préliminaires. 9. L'agent d'information et de soutien du PMC valide la demande d'adhésion. 10. L'agent d'information et de soutien du PMC vérifie que toute l'information exigée a été reçue. Si toute l'information a été reçue, allez à l'étape 15. 11. L'agent d'information et de soutien du PMC détermine si la demande doit être rejetée en raison de pièces manquantes. Si la demande est rejetée, allez à l'étape 14. 12. Si la demande n'est pas rejetée, l'agent d'information et de soutien du PMC réclame les informations manquantes au demandeur. 13. Le postulant fournit les informations manquantes. Allez à l'étape 9. 14. Si la demande est rejetée à l'étape 11, l'agent d'information et de soutien du PMC informe le demandeur que sa demande a été rejetée. Allez à l'étape 49. 15. Si toute l'information est reçue, le commis de soutien du PMC termine la saisie des données liées à la demande. 16. L'agent d'information et de soutien du PMC effectue un contrôle de la qualité des données entrées. 17. L'agent d'information et de soutien du PMC étudie l'évaluation de sécurité du demandeur dans le cadre de sa demande. 18. L'agent d'information et de soutien du PMC informe le demandeur que l'inscription au PMC est en cours. 19. L'agent d'information et de soutien du PMC demande des vérifications de sécurité (empreintes digitales, vérification nominale du casier judiciaire, vérification de la solvabilité, etc.), au besoin. 20. L'agent d'information et de soutien du PMC indique à l'unité d'apprentissage et de gestion du programme si le représentant désigné (RD) d'une organisation a besoin d'une formation. 21. Le processus de formation du PMC est déclenché. (Flux des travaux de la formation du représentant désigné sur le PMC 28). 22. Le responsable de l'inscription du PMC évalue la demande d'inscription et la confie pour traitement à un analyste de l'inscription du PMC. 23. L'analyste de l'inscription du PMC vérifie que la demande d'inscription et l'évaluation de sécurité sont complètes. 24. L'analyste de l'inscription du PMC s'assure que toute l'information requise a été reçue. Si toute l'information requise a été reçue, passez à l'étape 27. 25. L'analyste de l'inscription du PMC demande les informations manquantes au demandeur. 26. Le demandeur fournit les informations manquantes. Passez à l'étape 23. 27. L'analyste de l'inscription du PMC effectue la saisie des données de l'inscription. 28. L'analyste de l'inscription du PMC examine la demande d'inscription et l'évaluation de sécurité. 29. L'analyste de l'inscription du PMC détermine si un renvoi à l'unité d'analyse et de recherches (UAR) du PMC est requis. Si un renvoi n'est pas requis, passez à l'étape 31.

	30. Si un renvoi à l'UAR du PMC est requis, le processus de l'UAR du PMC est déclenché. (29 Flux des travaux de l'Unité d'analyse et de recherches [UAR] du PMC). Passez à l'étape 33. 31. L'analyste de l'inscription du PMC détermine si un renvoi à la Gestion des cas et pratiques exemplaires (GCPE) du PMC est requis. Si un renvoi à la GCPE du PMC n'est pas requis, passez à l'étape 33. 32. Si un renvoi à la GCPE du PMC est requis, le processus de la GCPE du PMC est déclenché (34 flux des travaux de la GCPE du PMC). Passez à l'étape 33. 33. L'analyste de l'inscription du PMC reçoit tous les résultats des précédentes étapes et détermine si la demande d'inscription au PMC sera approuvée, rejetée ou si le cas présente un risque élevé. Si la demande d'inscription au PMC est rejetée, passez à l'étape 35. Si la demande d'inscription au PMC est approuvée, passez à l'étape 39. 34. Si la demande d'inscription au PMC présente un risque élevé, l'analyste de l'inscription du PMC transmet la demande à un niveau supérieur. 35. Le gestionnaire des opérations du PMC évalue le renvoi à un niveau supérieur et prend la décision de rejeter ou d'approuver la demande d'inscription au PMC. Passez à l'étape 33. 36. Si la demande d'inscription au PMC est rejetée, l'analyste de l'inscription du PMC crée un formulaire de rejet. 37. Le directeur de l'inscription du PMC assure le contrôle de la qualité du formulaire de rejet. 38. Si le contrôle de la qualité du formulaire de rejet est un succès, passez à l'étape 49. Si le contrôle de la qualité du formulaire de rejet est un échec, il incombera à l'analyste de l'inscription du PMC d'y apporter des corrections. Passez à l'étape 36. 39. Si la demande d'inscription au PMC est approuvée, l'analyste de l'inscription du PMC crée un formulaire d'approbation. 40. Le directeur de l'inscription du PMC assure le contrôle de la qualité du formulaire d'approbation. 41. Si le contrôle de la qualité du formulaire d'approbation est un échec, il incombera à l'analyste de l'inscription du PMC d'y apporter des corrections. Passez à l'étape 39. 42. Si le contrôle de la qualité du formulaire d'approbation est un succès, le directeur de l'inscription du PMC saisit quelques données d'importance mineure. 43. Le directeur de l'inscription du PMC active les sites de l'organisation dans le système opérationnel du PMC. 44. Le directeur de l'inscription du PMC approuve l'organisation et les évaluations individuelles de sécurité requises. 45. L'analyste de l'inscription du PMC saisit les dernières données. 46. L'analyste de l'inscription du PMC crée une demande d'inspection, ce qui déclenche le flux des travaux des inspections du PMC. 47. Le flux des travaux des inspections du PMC est déclenché (30 flux des travaux des inspections du PMC). 48. L'analyste de l'inscription du PMC crée une trousse de correspondance sur l'inscription et l'envoie à l'organisation. 49. Fin du processus.
Intrants	• Demande de renouvellement d'inscription de l'organisation • Demandes individuelles d'évaluation de sécurité • Vérifications de sécurité • Autres documents justificatifs
Extrants	• Acceptation ou rejet de la demande d'inscription au PMC • Trousse d'inscription au PMC

	• Déclenchement de divers autres processus du PMC, tels que le processus de formation du PMC, le processus de l'UAR du PMC, etc.

1.2.4 Inscription au Programme des marchandises contrôlées - Formation du représentant désigné

Identification du flux des travaux	**28 Flux de travail de la formation du RD du PMC.**
Unité(s) opérationnelle(s)	• Organisation qui s'inscrit (Stagiaire) • Agent d'information du soutien du PMC • Gestion de programmes et Apprentissage (GPA) du PMC
Objectif opérationnel	• Formation des représentants désignés (RD).
Élément déclencheur	• Avant de pouvoir s'inscrire au PMC, l'organisation est tenue de nommer au moins un représentant désigné et de faire en sorte qu'il ait obtenu la certification des représentants désignés du PMC.
Description du flux des travaux	Début du processus. 1. GPA du PMC a été informée qu'une personne a besoin de suivre la formation de RD. 2. GPA du PMC écrit au stagiaire pour lui demander de s'inscrire au cours du Programme de certification des représentants désignés (PCRD). 3. Le stagiaire remplit l'inscription au cours. 4. Le stagiaire dispose de 30 jours pour s'inscrire au cours. 5. GPA du PMC reçoit toutes les inscriptions au cours du PCRD. 6. GPA du PMC consigne les renseignements relatifs à l'inscription au cours. 7. GPA du PMC examine et valide les renseignements sur l'inscription au cours afin de s'assurer que la personne inscrite est bien celle qui a été invitée à suivre le cours. Si les renseignements relatifs à l'inscription ne sont pas valides, passez à l'étape 17. 8. GPA du PMC consigne les inscriptions au cours validées. 9. GPA du PMC envoie des instructions au stagiaire sur la manière de récupérer la trousse de formation avant le début des cours. 10. Le stagiaire reçoit un courriel l'invitant à se préparer au cours. Si le stagiaire se voit offrir la possibilité de passer l'examen directement, et s'il décide de procéder ainsi, passez à l'étape 13. 11. Si le stagiaire décide de ne pas passer l'examen directement, il doit suivre les instructions fournies et accéder à WebEx pour télécharger la documentation du cours.

	12. Le stagiaire suit la formation du PCRD. 13. Le stagiaire passe l'examen du PCRD. 14. GPA du PMC corrige et note l'examen. 15. GPA du PMC consigne la note obtenue. Si le stagiaire échoue à l'examen lors de sa première tentative, passez à l'étape 20. Si le stagiaire échoue à l'examen à de nombreuses reprises, passez à l'étape 25. 16. GPA du PMC informe le stagiaire qu'il a réussi l'examen et que son certificat de RD lui sera envoyé une fois que l'organisation aura rempli l'inscription. 17. GPA du PMC examine l'inscription au cours et constate que le stagiaire qui s'est inscrit n'est pas personne qui avait été invitée à suivre le cours, l'inscription au cours est rejetée. 18. GPA du PMC rejette l'inscription au cours. 19. GPA du PMC informe la personne qu'elle n'est pas admissible à suivre la formation du PCRD. 20. GPA du PMC informe le stagiaire qu'il a échoué à l'examen, et qu'il doit se prévaloir de l'une des deux options suivantes, à savoir, reprendre l'examen ou refaire la formation. 21. Le stagiaire décide de repasser l'examen. 22. Le stagiaire s'inscrit à l'examen seulement. 23. Le stagiaire informe GPA du PMC de sa décision de repasser l'examen. 24. Le stagiaire décide de suivre de nouveau la formation, passez à l'étape 2. 25. GPA du PMC informe le stagiaire qu'il a échoué à l'examen à de trop nombreuses reprises, et qu'il doit suivre de nouveau la formation, passez à l'étape 2. 26. Le stagiaire décide de ne pas suivre le cours, il avise GPA du PMC d'annuler sa présente inscription au cours. 27. GPA du PMC annule l'inscription du stagiaire. 28. GPA du PMC consigne le fait que le stagiaire a annulé la formation. Si le stagiaire a toujours besoin de suivre la formation, le processus reprend depuis le début, passez à l'étape 1. 29. Fin du processus.
Intrants	• Nouvelle demande d'inscription avec l'identification du RD.
Extrants	• Certification du RD.

1.2.5 Analyse et recherches

Identification du flux des travaux	29 Flux des travaux du renvoi pour motif valable du PMC
Unité(s) opérationnelle(s)	• Analyste de l'inscription au PMC • Inspecteur du PMC • Gestion de cas et des pratiques exemplaires (GCPE) du PMC • Analyste de l'unité d'analyse et de recherches (UAR) du PMC • Organisations partenaires du PMC (p. ex., GRC, SCRS, etc.)
Objectif opérationnel	• Évaluer les évaluations de sécurité des organisations et des personnes, effectuer des analyses et consulter les organisations partenaires du PMC en vue de formuler une recommandation concernant l'organisation ou la personne dans l'éventualité où l'analyste de l'inscription ou l'inspecteur du PMC serait incapable d'effectuer une analyse satisfaisante ou s'il existe un risque élevé.
Élément déclencheur	• Les renvois pour motif valable sont déclenchés dans le cadre du processus d'inscription ou d'inspection.
Description du flux des travaux	Début du processus. 1. L'analyste de l'inscription ou l'inspecteur du PMC présente une demande de renvoi pour motif valable y compris toute la documentation à l'appui. 2. L'analyste de l'UAR du PMC procède à une évaluation initiale du renvoi pour motif valable en vue de déterminer s'il est pertinent, valide et justifié. Si l'analyste de l'UAR du PMC détermine que le « renvoi pour motif valable » n'est pas valide, passez à l'étape 5. 3. L'analyste de l'UAR du PMC fait l'analyse du renvoi pour motif valable, et prend une décision concernant l'incidence et le risque. Si l'incidence et le risque sont élevés, le processus de GCPE est déclenché, passez à l'étape 9, sinon, continuez jusqu'à l'étape 6. 4. L'analyste de l'UAR du PMC présente le renvoi aux organisations partenaires du PMC à des fins d'évaluation. Les organisations partenaires du PMC sont notamment la GRC, le SCRS, etc. 5. L'analyste de l'UAR du PMC annule le renvoi pour motif valable, passez à l'étape 7. 6. À la suite de l'analyse du renvoi pour motif valable de l'UAR du PMC à l'étape 3, l'UAR du PMC formule une recommandation concernant le renvoi. 7. L'analyste de l'UAR du PMC informe l'auteur du renvoi pour motif valable (34 Flux des travaux de la GCPE du PMC) de la décision que le renvoi n'était pas requis ou de leurs recommandations. 8. L'inscription du PMC ou l'inspection du PMC reçoit l'avis d'annulation ou l'avis de recommandation de l'UAR du PMC.

	9. Le processus de GCPE du PMC est déclenché. Le renvoi pour motif valable est renvoyé à la division de la GCPE du PMC. Une demande serait renvoyée si elle était jugée à risque élevé ou s'il subsistait une inquiétude non dissipée de la part de l'analyste de l'UAR du PMC. 10. Fin du processus.
Intrants	• Demande de renvoi pour motif valable • Justification du renvoi • Évaluation du partenaire du PMC
Extrants	• Demande d'évaluation par un partenaire du PMC • Renvoi du renvoi pour motif valable à la GCPE du PMC.

1.2.6 Inspection

Identification du flux des travaux	**30 Inspections du flux des travaux du Programme des marchandises contrôlées (PMC)**
Unité(s) opérationnelle(s)	• Organisme de l'industrie • Inscription au PMC • Gestion du PMC • Gestion de cas et des pratiques exemplaires (GCPE) du PMC • Unité d'analyse et de recherches (UAR) du PMC • Agent de conformité au contrôle de la qualité du PMC • Inspecteur de conformité (inspecteur) du PMC • Coordonnateur de conformité des voyages du PMC • Gestionnaire d'inspection de conformité du PMC
Objectif opérationnel	• Compléter une inspection déclenchée par le PMC.
Élément déclencheur	• Une inspection peut être déclenchée à la suite du processus d'inscription (inscription nouvelle, renouvelée ou modifiée), d'une demande de résiliation, d'une inspection ponctuelle demandée par la gestion du PMC, d'un incident ou de la violation d'une demande d'inspection dans le cadre d'une enquête ou d'une inspection de suivi en raison de lacunes en matière de conformité découvertes lors d'une inspection précédente.
Description du flux des travaux	Début du processus. 1. L'agent de conformité au contrôle de la qualité du PMC examine et classe la demande d'inspection reçue.

	2. L'agent de conformité au contrôle de la qualité du PMC examine la liste des demandes d'inspection non attribuées qui sont triées par emplacement d'inspection. 3. L'agent de conformité au contrôle de la qualité du PMC détermine si la demande d'inspection peut être reportée. Si la demande d'inspection ne peut pas être reportée, passez à l'étape 8. 4. L'agent de conformité au contrôle de la qualité du PMC prépare la recommandation de report. 5. Le gestionnaire d'inspection de conformité examine la recommandation de report. 6. Si le gestionnaire d'inspection de conformité n'approuve pas la recommandation de report, passez à l'étape 8. 7. Si le gestionnaire d'inspection de conformité approuve la recommandation de report, l'agent conformité au contrôle de la qualité reporte la demande d'inspection non attribuée. Retournez à l'étape 2. 8. L'agent de conformité au contrôle de la qualité examine les calendriers individuels des membres de l'équipe d'inspection. 9. L'agent de conformité au contrôle de la qualité attribue la demande à un inspecteur de conformité du PMC selon la priorité de la demande d'inspection, la date d'agenda la plus rapprochée et l'emplacement géographique semblable pour créer un bloc de demande d'inspection. La date de l'agenda correspond à la date à laquelle l'inscription est accordée. Il faut 90 jours pour une nouvelle inscription. 10. L'agent de conformité au contrôle de la qualité du PMC répète ce processus jusqu'à ce qu'il n'y ait plus de demande d'inspection non attribuée et il recommence à l'étape 2, sinon il poursuit. 11. L'agent de conformité au contrôle de la qualité examine la liste des inspections reportées afin de déterminer celles qui pourraient être utilisées pour compléter un bloc de demande d'inspection. 12. L'agent de conformité au contrôle de la qualité annule le report de cette demande d'inspection et l'assigne à un inspecteur de conformité du PMC. 13. L'agent de conformité au contrôle de la qualité répète ce processus jusqu'à ce que le bloc de demande d'inspection de l'inspecteur de conformité du PMC soit complet. S'il reste de la disponibilité dans le bloc de demande d'inspection, passez à l'étape 6, sinon continuez. 14. L'inspecteur de conformité du PMC examine la demande d'inspection attribuée. 15. Au besoin, l'inspecteur de conformité du PMC peut présenter une demande à l'agent de conformité au contrôle de la qualité pour qu'une inspection soit attribuée à un autre inspecteur ou soit reportée. 16. L'inspecteur de conformité du PMC détermine si la demande d'inspection peut être effectuée par téléphone ou si elle doit être effectuée sur place. Si une inspection sur place est requise, passez à l'étape 17. 17. Si l'inspection peut être effectuée au téléphone, l'inspecteur de conformité du PMC communique avec l'organisme pour mener l'inspection téléphonique. 18. Si l'inspecteur de conformité du PMC parvient à effectuer l'inspection téléphonique, passez à l'étape 52. 19. Si l'inspecteur de conformité du PMC est incapable de communiquer avec l'organisme après de nombreux essais, il doit envoyer un courriel à la personne ressource de l'organisme pour convenir de la date et de l'heure auxquelles l'inspection téléphonique peut être effectuée. Passez à l'étape 16. Si l'inspecteur de conformité du PMC a pu entrer en contact avec l'organisme, passez à l'étape 13.

	20. Si l'inspecteur de conformité du PMC n'est pas en mesure d'effectuer l'inspection téléphonique dans un délai raisonnable, il présente une demande à l'agent de conformité au contrôle de la qualité pour suspendre la demande d'inspection le temps d'obtenir les renseignements. Cette mesure arrêtera le temps lié au service pour la demande d'inspection. 21. Si l'inspecteur de conformité du PMC est toujours incapable d'entrer en contact avec l'organisme, il élabore un renvoi à la GCPE, puis déclenche le processus de GCPE du PMC (34 Flux des travaux de la GCPE du PMC). 22. L'inspecteur de conformité du PMC ajoute l'inspection à son calendrier d'inspections et entre une date et une heure d'inspection prévues provisoirement pour la demande. 23. L'inspecteur de conformité du PMC détermine si son bloc de demande d'inspection pour les inspections sur place est complet. S'il ne l'est pas, retournez à l'étape 9 pour examiner une autre demande d'inspection. 24. Une fois que le bloc de demande d'inspection pour les inspections sur place est jugé complet, l'inspecteur de conformité du PMC élabore un itinéraire de voyage provisoire qui sera présenté au coordonnateur de conformité des voyages du PMC pour approbation. 25. Le coordonnateur de conformité des voyages du PMC approuve l'itinéraire de voyage et organise les préparatifs de voyage au nom de l'inspecteur de conformité du PMC. 26. L'inspecteur de conformité du PMC envoie des courriels à la personne ressource des organisations pour se présenter et fixer une date et une heure pour l'inspection. 27. L'inspecteur de conformité du PMC communique avec la personne ressource de l'organisation par téléphone ou par courriel pour obtenir des réponses aux questions contenues dans la liste de vérification de conformité avant inspection du PMC. 28. En fonction des réponses obtenues aux questions de la liste de vérification avant inspection, si l'inspecteur de conformité de PMC détermine qu'il n'y a pas de marchandises contrôlées sur place, il remplace l'inspection sur place par une inspection par téléphone, passez à l'étape 52. 29. En fonction des réponses obtenues aux questions de la liste de vérification avant inspection, l'inspecteur de conformité du PMC détermine s'il y a des modifications à apporter à la demande d'inscription au PMC du demandeur. Si l'inspecteur de conformité du PMC détermine qu'il n'y a pas de modification à apporter à la demande, passez à l'étape 26. 30. L'inspecteur de conformité du PMC fournit à la personne ressource de l'organisme une copie vierge d'une demande d'inscription qui doit être complétée et retournée au PMC. 31. Si, après avoir communiqué avec la personne ressource de l'organisation, il est impossible de fixer une date et une heure (dans un délai raisonnable), l'inspecteur de conformité du PMC avisera l'agent de conformité au contrôle de la qualité de désattribuer la demande d'inspection et il fournira une date ultérieure au moment où l'inspection peut être effectuée. Passez à l'étape 2. 32. L'inspecteur de conformité du PMC envoie un courriel à la personne ressource de l'organisme pour confirmer la date et l'heure qui étaient prévues pour l'inspection. 33. L'inspecteur de conformité du PMC doit remplir les sections 1 à 6 de la liste de vérification avant inspection. Si ces sections de la liste de vérification avant inspection (1 à 6) ne peuvent pas être remplies, l'inspecteur de conformité du PMC doit communiquer à nouveau avec l'organisme. Passez à l'étape 21. 34. Si la liste de vérification avant inspection (sections 1 à 6) est remplie, l'inspecteur de conformité du PMC peut confirmer l'inspection dans son bloc de demandes d'inspection. Cette tâche doit être exécutée pour toutes les demandes d'inspection

	attribuées du bloc d'inspection. Ensuite, l'inspecteur de conformité du PMC envoie un avis de bloc d'inspection définitif au gestionnaire des inspections de conformité et à l'agent de conformité au contrôle de la qualité. 35. L'inspecteur de conformité du PMC demande les dossiers d'inscription de la salle des dossiers pour toutes les entités inscrites dans son bloc de demandes d'inspection. 36. L'inspecteur de conformité du PMC reçoit les dossiers d'inscription. 37. L'inspecteur de conformité du PMC complète les sections 7 à 10 de la liste de vérification avant inspection pour les demandes d'inspections qui se trouvent dans son bloc de demande d'inspection. 38. L'inspecteur de conformité du PMC confirme l'approbation de voyage. Si l'approbation de voyage n'a pas été obtenue, il essaie de l'obtenir. 39. L'inspecteur de conformité du PMC mène l'inspection. 40. Il remplit le questionnaire d'inspection. 41. Il remplit le formulaire d'inspection de conformité. 42. Il complète les activités après inspection. Si aucune lacune n'a été découverte pendant l'inspection des lieux, l'inspecteur de conformité du PMC présente un rapport d'inspection à l'agent de conformité au contrôle de la qualité. Passez à l'étape 49. 43. L'inspecteur de conformité du PMC avise l'organisme de lacunes repérées pendant l'inspection et convient avec lui d'un délai raisonnable dans lequel les lacunes doivent être corrigées. 44. Si les lacunes n'ont toujours pas été corrigées à la date convenue, passez à l'étape 47. 45. L'inspecteur de conformité du PMC doit déterminer si un suivi d'inspection est nécessaire. Si aucun suivi d'inspection n'est nécessaire, l'inspecteur de conformité du PMC présente le rapport d'inspection à l'agent de conformité au contrôle de la qualité. Passez à l'étape 49. 46. Si un suivi d'inspection est nécessaire, l'inspecteur de conformité du PMC doit présenter une demande de suivi d'inspection qui est traitée comme une nouvelle demande d'inspection. Passez à l'étape 2. 47. Si les lacunes repérées ne sont pas corrigées d'ici la date convenue, l'inspecteur de conformité du PMC doit déterminer si un transfert à la GCPE est nécessaire. Si aucun renvoi n'est nécessaire, l'inspecteur de conformité du PMC présente le rapport d'inspection à l'agent de conformité au contrôle de la qualité. Passez à l'étape 49. 48. L'inspecteur de conformité élabore un rapport de GCPE qui déclenche ensuite le processus de GCPE du PMC (34 Flux des travaux de la GCPE du PMC). 49. L'agent de conformité au contrôle de la qualité effectue un contrôle de la qualité sur le rapport d'inspection. Si le contrôle est réussi, passez à l'étape 52. 50. Si le contrôle de la qualité n'est pas réussi, l'agent de conformité au contrôle de la qualité retourne le rapport d'inspection à l'inspecteur de conformité du PMC pour qu'il le corrige. 51. L'inspecteur de conformité du PMC met à jour le rapport d'inspection et le présente à nouveau au contrôle de la qualité. Passez à l'étape 49. 52. Fin du processus.
Intrants	• Demande d'inspection provenant de divers facteurs déclencheurs • Liste de vérification pour l'inspection • Questionnaire pour l'inspection

Extrants	• L'entité inscrite est jugée conforme • L'inspection a permis de découvrir des lacunes en matière de conformité qui demandent des mesures • L'entité inscrite est jugée non conforme • Renvoi à la GCPE • Rapport d'inspection

1.2.7 Exemptions relatives aux travailleurs temporaires

Identification du flux des travaux	31 Exemption du flux des travaux du PMC relative aux travailleurs temporaires
Unité(s) opérationnelle(s)	• Représentant désigné (RD) de l'organisme qui s'inscrit • Analyste de l'unité d'analyse et de recherches (UAR) du PMC • Gestion de cas et des pratiques exemplaires (GCPE) du PMC • Organisations partenaires du PMC (p. ex., GRC, SCRS, etc.)
Objectif opérationnel	• Procéder à l'exemption des travailleurs temporaires d'une organisation inscrite au PMC pour que les travailleurs temporaires n'aient pas besoin de s'inscrire au PMC, mais puissent quand même être exposés aux marchandises contrôlées.
Élément déclencheur	• Le RD d'une organisation inscrite au PMC présente une demande d'exemption relative à un travailleur temporaire.
Description du flux des travaux	Début du processus. 1. Le RD de l'organisation présente un dossier de demande relatif à un travailleur temporaire. 2. L'analyse de l'UAR du PMC reçoit le dossier de demande relatif à un travailleur temporaire et effectue une première analyse afin d'évaluer la pertinence, la validité et la raison de la demande. Si la demande est valide, passez à l'étape 4. 3. Si l'analyste de l'UAR détermine que la demande est incomplète, qu'aucune exemption n'est nécessaire ou que la demande est annulée par le RD, il doit aviser le RD et les originaux ou les copies des documents à l'appui sont retournés au RD. Passez à l'étape 11. 4. L'analyste de l'UAR présente un renvoi aux organisations partenaires de PMC à des fins d'évaluation. 5. L'analyste de l'UAR effectue une analyse approfondie de la demande relative au travailleur temporaire en plus de l'analyse des partenaires. 6. Si l'analyste de l'UAR détermine que la demande représente un risque élevé ou s'il y a une préoccupation non résolue, la demande est transférée à la GCPE du PMC. 7. Le processus de GCPE du PMC est déclenché (34 Flux des travaux de la GCPE du PMC).

	8. L'analyste de l'UAR approuve l'exemption relative au travailleur temporaire sans condition, crée le certificat d'exemption et le fait parvenir au RD. 9. L'analyste de l'UAR approuve l'exemption relative au travailleur temporaire sous certaines conditions, élabore le certificat d'exemption et les conditions requises (comme l'accès restreint à certaines zones du lieu de travail) et le fait parvenir au RD. 10. L'analyse de l'UAR détermine que l'exemption relative au travailleur temporaire doit être refusée. Le RD est avisé du refus. 11. Fin du processus.
Intrants	• Demande d'exemption d'inscription au PMC – Formulaire relatif aux travailleurs temporaires • Formulaire d'évaluation de sécurité des travailleurs temporaires • Copie du permis de travail délivré par Citoyenneté et Immigration Canada. • Exemplaire original d'un certificat de bonne conduite • Copie de passeport valide
Extrants	• Décision d'exemption relative au travailleur temporaire (approuvée, retournée, refusée, etc.) • Certificat d'exemption relative au travailleur temporaire (possiblement sous certaines conditions selon la situation) pour les travailleurs temporaires approuvés. • Lettre d'exemption • Lettre de refus

1.2.8 Exemptions accordées aux visiteurs

Identification du flux des travaux	**32 Exemption du flux des travaux du PMC accordée aux visiteurs**
Unité(s) opérationnelle(s)	• Représentant désigné (RD) de l'organisme qui s'inscrit • Analyste de l'unité d'analyse et de recherches (UAR) du PMC • Gestion de cas et des pratiques exemplaires (GCPE) du PMC
Objectif opérationnel	• Procéder à l'exemption des visiteurs d'une organisation inscrite au PMC pour que les visiteurs temporaires n'aient pas besoin de s'inscrire au PMC, mais puissent quand même être exposés aux marchandises contrôlées.
Élément déclencheur	• Le RD d'une organisation inscrite au PMC présente une demande d'exemption relative à un visiteur.
Description du flux des travaux	Début du processus. 1. Le RD de l'organisation présente un dossier de demande relatif à un visiteur.

	2. L'analyse de l'UAR du PMC reçoit le dossier de demande relatif à un visiteur et effectue une première analyse afin d'évaluer la pertinence, la validité et la raison de la demande. Si la demande est valide, passez à l'étape 4. 3. Si l'analyste de l'UAR détermine que la demande est incomplète, qu'aucune exemption n'est nécessaire ou que la demande est annulée par le RD, il doit aviser le RD et les originaux ou les copies des documents à l'appui sont retournés au RD. Passez à l'étape 9. 4. L'analyste de l'UAR effectue une analyse approfondie de la demande du visiteur. 5. Si l'analyste de l'UAR détermine que la demande représente un risque élevé ou s'il y a une préoccupation non résolue, la demande est transférée à la GCPE du PMC. Le processus de GCPE du PMC est déclenché (34 Flux des travaux de la GCPE du PMC). 6. L'analyste de l'UAR approuve l'exemption relative au visiteur sans condition, crée le certificat d'exemption et le fait parvenir au RD. 7. L'analyste de l'UAR approuve l'exemption relative au visiteur sous certaines conditions, élabore le certificat d'exemption et les conditions requises (comme l'accès restreint à certaines zones du lieu de travail) et le fait parvenir au RD. 8. L'analyse de l'UAR détermine que l'exemption relative au visiteur doit être refusée. Le RD est avisé du refus. 9. Fin du processus.
Intrants	• Demande du visiteur pour le formulaire d'exemption • Copie de passeport valide • Copie du permis d'exportation valide, le cas échéant
Extrants	• Renvoi à la GCPE • Certificat d'exemption (sous certaines conditions requises) pour les visiteurs approuvés • Lettre d'exemption • Lettre de refus

1.2.9 Recommandation d'employé de l'industrie

Identification du flux des travaux	**33 Recommandation d'employé de l'industrie du flux des travaux du PMC**
Unité(s) opérationnelle(s)	• Représentant désigné (RD) de l'organisme qui s'inscrit • Analyste de l'unité d'analyse et de recherches (UAR) du PMC • Gestion de cas et des pratiques exemplaires (GCPE) du PMC • Organisations partenaires du PMC (p. ex., GRC, SCRS, etc.)
Objectif opérationnel	• Le RD est responsable de réaliser des évaluations de sécurité des employés, des administrateurs et des cadres, ainsi que de déterminer le niveau de risque de transfert lié à ses employés, administrateurs et cadres. Le PMC fournit au RD une Procédure

	d'évaluation de la gestion des risques qui est utilisée pour mener des évaluations de sécurité. Les recommandations des employés sont évaluées par l'analyste de l'UAR et une recommandation de décision est retournée au RD.
Élément déclencheur	• Le RD est incapable de mener l'évaluation de sécurité de manière satisfaisante pour un employé ou le niveau de risque est jugé suffisamment élevé.
Description du flux des travaux	Début du processus. 1. Le RD de l'organisation présente un dossier de demande de recommandation d'un employé 2. L'analyse de l'UAR du PMC reçoit le dossier de demande de recommandation de l'employé et effectue une première analyse afin d'évaluer la pertinence, la validité et la raison de la demande. Si la demande est valide, passez à l'étape 4. 3. Si l'analyste de l'UAR détermine que la recommandation est incomplète, qu'aucune recommandation n'est nécessaire ou qu'elle est annulée par le RD, il doit aviser le RD et les originaux ou les copies des documents à l'appui sont retournés au RD. Passez à l'étape 10. 4. L'analyste de l'UAR présente un renvoi aux organisations partenaires de PMC à des fins d'évaluation. 5. L'analyste de l'UAR effectue une analyse approfondie de la demande de recommandation de l'employé en plus de l'analyse des partenaires. 6. Si l'analyste de l'UAR détermine que la demande de recommandation de l'employé représente un risque élevé ou s'il y a une préoccupation non résolue, la demande est transférée à la GCPE du PMC. 7. Le processus de GCPE du PMC est déclenché (34 Flux des travaux de la GCPE du PMC). 8. L'analyse de l'UAR confirme l'évaluation des risques du RD. L'analyste de l'UAR élabore la lettre de recommandation et la fait parvenir au RD. 9. L'analyse de l'UAR modifie l'évaluation des risques du RD. L'analyste de l'UAR élabore la lettre de recommandation et la fait parvenir au RD. 10. Fin du processus.
Intrants	• Évaluation de sécurité de l'employé effectuée par le RD • Exemplaire original d'un certificat de bonne conduite • Preuve de citoyenneté • Motif de la recommandation
Extrants	• Lettre de recommandation

1.2.10 Gestion des cas et pratiques exemplaire

Identification du flux des travaux	34 Flux des travaux de la GCPE du PMC
Entité(s)	• Organisation de l'industrie • Inscription au PMC • Gestion du PMC • Gestion des cas et pratiques exemplaires (GCPE) du PMC • Unité d'analyse et de recherches (UAR) du PMC • Agent de conformité au contrôle de la qualité du PMC • Inspecteur de conformité (inspecteur) du PMC • Organismes politiques • Grand public
Objectif opérationnel	• Mener à bien une enquête amorcée sur la gestion des cas et pratiques exemplaires (GCPE) du PMC.
Élément déclencheur	• Une enquête sur la GCPE peut être déclenchée à la suite de tout autre processus du PMC. • Les enquêtes sur la GCPE sont déclenchées selon les besoins.
Description du flux des travaux	1. Début du processus. 2. Une demande de renvoi sur la GCPE est soumise à la GCPE. 3. Le gestionnaire de la GCPE examine et confie le renvoi à un agent de la gestion des cas. 4. L'agent de la gestion des cas de la GCPE crée un dossier. 5. L'agent de la gestion des cas de la GCPE détermine si une violation a été commise. Si une violation a été commise, continuez à l'étape 6, sinon passez à l'étape 25. 6. L'agent de la gestion des cas de la GCPE lance des procédures d'enquête selon la nature du renvoi. Les types de renvois comprennent les infractions à la *Loi sur la production de défense*, les omissions, les risques injustifiés, les problèmes de conformité, etc. 7. L'agent de la gestion des cas détermine si la plainte présentée dans le renvoi est fondée. Si la plainte est fondée, poursuivez à l'étape suivante, sinon allez à l'étape 13. 8. Le gestionnaire de la GCPE rédige une lettre d'intention décrivant la plainte et les étapes à suivre pour résoudre le problème. 9. L'agent de la gestion des cas de la GCPE adresse la lettre d'intention à la personne inscrite. 10. Si de nouvelles informations concernant la plainte sont reçues, passez à l'étape 11, sinon passez à l'étape 14. 11. L'agent de la gestion des cas de la GCPE effectue les analyses des informations nouvellement reçues.

	12. L'agent de la gestion des cas de la GCPE détermine si une décision favorable peut être prise concernant la plainte. Si aucune décision favorable ne peut être prise, allez à l'étape 14. Sinon, continuez à l'étape 13. 13. L'agent de la gestion des cas de la GCPE renseigne la DMC sur le dénouement de la plainte. Passez à l'étape 25. 14. Le gestionnaire de la GCPE rédige une recommandation pour le directeur du PMC afin de suspendre la personne inscrite. 15. Le directeur du PMC examine et évalue la recommandation de suspension. 16. Le directeur du PMC détermine si une décision favorable peut être prise concernant la suspension. Si aucune décision favorable ne peut être prise, passez à l'étape 19. Sinon, passez à l'étape suivante. 17. L'agent de la gestion des cas de la GCPE peut rétablir la personne inscrite ou faire une demande d'exemption. 18. L'agent de la gestion des cas de la GCPE informe la personne inscrite de sa suspension. Passez à l'étape 25. 19. Le gestionnaire de la GCPE rédige une recommandation pour le directeur du PMC afin de révoquer la personne inscrite. 20. Le directeur du PMC examine et évalue la recommandation de révocation. 21. Le directeur du PMC détermine si une décision favorable peut être prise concernant la révocation. Si aucune décision favorable concernant la révocation ne peut être prise, passez à l'étape 17. Sinon, passez à l'étape 22. 22. L'agent de la gestion des cas de la GCPE informe la personne inscrite de sa révocation. 23. L'agent de la gestion des cas de la GCPE avise l'inspection du PMC de la nécessité d'effectuer une inspection de clôture. 24. Le processus d'inspection du PMC est déclenché (30 flux des travaux des inspections du PMC). 25. L'agent de la gestion des cas de la GCPE clôt le dossier de la GCPE et crée un rapport de la GCPE. 26. Fin du processus.
Intrants	• Demande de renvoi à la GCPE
Extrants	• Rapport de la GCPE. • Lettre d'intention pour suspension ou révocation. • Recommandation de suspension. • Rétablissement auprès de la DMC. • Inspection de clôture.

APPENDICE 2 DE L'ANNEXE A – ACTIVITÉS PRINCIPALES

APPENDICE 2 DE L'ANNEXE A – ACTIVITÉS PRINCIPALES

Le présent appendice décrit une série d'Activités principales et les dates d'achèvement qui y sont associées. Le calendrier ci-dessous reflète les attentes et l'approche proposée, qui comprend des activités continues de communication, d'essais et de formation pendant la conception et le développement du système, un projet pilote du système et la mise en œuvre progressive du système pour ses parties intéressées. Les dates de livraison des jalons du projet seront assujetties à l'attribution du contrat et à la date de début de l'entrepreneur. Si des retards surviennent dans l'attribution d'un contrat, les dates des jalons du projet seront ajustées en conséquence. L'ajustement du calendrier, le cas échéant, se fera lors de l'attribution du contrat.

Activités principales	Date d'achèvement
Attribution du contrat	Août 2017
Planification de la solution et analyse	Décembre 2017
Conception de la solution	Décembre 2017
Communication	Mars 2019 [1]
Essais	Mars 2019 [1]
Formation	Mars 2019 [1]
Développement et configuration de la solution	Août 2018
Préparation opérationnelle	Mars 2019
Mise en œuvre et lancement du projet pilote de solution	Mars 2019
Projet pilote de solution	Juin 2019
Mise en œuvre progressive	Septembre 2019
Stabilisation de la solution et transition de sortie	Décembre 2019
Clôture du projet	Décembre 2019

[1] Les communications, les essais et la formation doivent commencer dès que possible, être récurrents et être adaptés selon les publics cibles.

Vous trouverez ci-dessous un aperçu de très haut niveau du déroulement prévu du projet. Les différentes étapes du cycle de développement habituel des logiciels sont décrites en termes généraux, afin de donner une idée de la façon dont l'entrepreneur et SPAC interagiront pendant le développement et la mise en œuvre de la solution. Il est à noter que les étapes ci-dessous montrent une séquence suivant une méthode en cascade. Toutefois, il est entendu que certaines étapes et activités seront réalisées en parallèle.

Pour assurer la mise en œuvre efficace de la solution, il sera nécessaire d'adopter, tout au long du cycle de vie du projet, une approche cyclique de la formation, des essais et des communications.

La réalisation de la solution commencera par le lancement de l'étape du projet pilote au cours de laquelle une partie de la solution sera mise à la disposition d'un certain nombre de personnes, ce qui permettra d'obtenir une évaluation finale de l'état préparation opérationnelle et de corriger tout problème éventuel dans un cas isolé. À la fin de la phase pilote, la solution sera mise en vigueur à l'aide de déploiements échelonnés, vu que le système sera présenté aux groupes d'intervenants progressivement. La mise en œuvre progressive permettra d'assurer la continuité des activités avec une transition graduelle entre les actuels systèmes de soutien aux activités du Secteur de la sécurité industrielle et la nouvelle solution. La mise en œuvre progressive permettra également à l'entrepreneur de régler les problèmes de façon contrôlée avant que l'intégralité de la solution entre en production.

L'entrepreneur doit produire, gérer, réviser et mettre en œuvre tous les produits livrables définis à l'ANNEXE A conformément aux jalons à l'annexe B. Tous les produits livrables demandés doivent être approuvés par le responsable du projet. Les produits livrables doivent être remis au responsable du projet à l'achèvement ou sur demande, à la discrétion du responsable du projet.

1. Lancement du projet

À l'attribution du contrat, le projet passera à l'étape de la réalisation. On s'attend à ce que l'entrepreneur et SPAC soient amenés à collaborer plus étroitement.

Dès l'attribution du contrat, l'entrepreneur doit :

(a) mettre sur pied une équipe de gestion du projet;
(b) fournir son modèle organisationnel;
(c) fournir un modèle de gouvernance;
(d) organiser une séance de lancement du projet.

2. Étape de planification

Pendant cette étape, l'entrepreneur et SPAC examineront les exigences et les processus opérationnels afin d'assurer une compréhension complète et exacte. La planification de la restructuration des processus opérationnels, des communications, de la formation, des essais et de la gestion du changement et du projet commencera. Les plans établis doivent comprendre les délais, les publics cibles, les risques potentiels et les stratégies d'atténuation connexes, ainsi qu'une description des activités, comme il est indiqué dans les exigences décrites à l'ANNEXE A. Les délais doivent concorder avec les Activités principales présentés ci-dessus.

À la fin de cette étape, l'entrepreneur doit :

(a) perfectionner les stratégies et les plans de communications et de gestion du changement;
(b) créer et fournir un registre des risques où seront détaillés les risques, les stratégies d'atténuation et les mesures prises à l'égard du projet;
(c) fournir un registre des problèmes où seront détaillés les problèmes rencontrés dans le cadre du projet et les mesures qui y sont associées;
(d) perfectionner le plan de gestion du projet;
(e) élaborer et fournir un échéancier global d'exécution des exigences du projet;
(f) fournir une stratégie et un plan de restructuration des processus opérationnels;
(g) fournir un plan de réalisation de la solution;
(h) fournir une stratégie et un plan de migration des données.

3. Étape d'analyse

Pendant cette étape, l'entrepreneur aura l'occasion de mettre à profit son expertise et sa connaissance de l'outil de gestion des cas ainsi que sa compréhension nouvellement acquise des exigences pour remettre en question les processus opérationnels et recommander des changements afin d'en d'améliorer l'efficacité et l'efficience.

À la fin de cette étape, l'entrepreneur doit :

(a) lancer les cycles de communication, d'essais, de formation et de gestion du changement;
(b) analyser et restructurer les processus opérationnels en leur état actuel;
(c) proposer des changements aux processus opérationnels et mettre à jour les schémas de processus opérationnels dès que SPAC les aura approuvés;
(d) élaborer l'architecture opérationnelle de la solution;

(e) contribuer au franchissement du point de contrôle 1 du processus d'évaluation et d'autorisation de sécurité, comme il est indiqué à la section 5, 1.1.1 de l'ANNEXE A;
(f) élaborer le plan de préparation opérationnelle;
(g) perfectionner le plan de migration des données;
(h) perfectionner le plan de restructuration des processus opérationnels;
(i) perfectionner le plan de réalisation de la solution;

4. Étape de conception

Après l'achèvement de l'étape d'analyse, l'entrepreneur doit perfectionner et détailler la conception de la solution. Il doit concevoir une architecture logique de la solution de technologie de l'information, en collaboration avec le Bureau de l'architecture d'entreprise de SPAC. L'architecture logique doit fournir plus de détails sur la solution à mettre en œuvre et traiter les perspectives de l'organisation, de l'application, des données, de la technologie et de l'architecture de sécurité. SPAC facilitera et coordonnera toutes les communications et toutes les activités avec Services partagés Canada, qui assurera le soutien et la responsabilité des éléments d'infrastructure, tels les centres de données, les serveurs, les réseaux et la sécurité de l'infrastructure.

L'entrepreneur doit :

(a) fournir l'architecture logique de la solution pour approbation par le Conseil d'examen de l'architecture de SPAC;
(b) exécuter le plan de contrôle de l'accès et de gestion des utilisateurs;
(c) mettre à jour le plan de gestion du projet;
(d) perfectionner les plans de communications, de formation et d'essais;
(e) perfectionner le plan de gestion du changement;

5. Étape d'élaboration

Après avoir terminé la conception du projet et l'avoir fait approuver, l'entrepreneur doit élaborer, configurer et intégrer la technologie selon les spécifications de l'architecture de la solution et les processus opérationnels approuvés. L'objectif est de configurer la solution selon les exigences énoncées à l'ANNEXE A et les exigences définies en détail et approuvées pendant les étapes de planification et de conception.

L'entrepreneur doit :

(a) perfectionner le plan d'essais et les cas d'essai conformément aux exigences de la solution touchant les essais du système, les essais d'acceptation par les utilisateurs, les essais de rendement et les essais de charge;
(b) élaborer et fournir des plans d'évaluation de la sécurité pour approbation;
(c) perfectionner le plan de préparation opérationnelle;
(d) fournir des spécifications de conception détaillées;
(e) perfectionner le plan de réalisation de la solution;
(f) perfectionner le plan de contrôle de l'accès et de gestion des utilisateurs;
(g) élaborer le plan de mise en œuvre du projet pilote de solution;

6. Étape d'essais

Conformément aux exigences d'essais énoncées à l'ANNEXE A, tous les essais doivent être terminés avant de mettre en œuvre la solution dans l'environnement de production. L'entrepreneur doit perfectionner le plan d'essais et les cas d'essai de la solution en fonction des exigences de la solution.

L'entrepreneur doit :

(a) exécuter le plan d'essais et soumettre pour approbation les résultats des essais du système, unitaires, fonctionnels, de bout en bout, de sécurité, de rendement et de charge;
(b) fournir la matrice de traçabilité des exigences dûment remplie;
(c) franchir le point de contrôle 2 du processus d'évaluation et d'autorisation de sécurité;

7. Étape de formation

Conformément aux exigences de formation énoncées à l'ANNEXE A, toutes les formations doivent être données avant de mettre en œuvre la solution dans l'environnement de production.

L'entrepreneur doit :

(a) exécuter le plan de formation;
(b) perfectionner le plan de préparation opérationnelle;
(c) procéder à l'évaluation de l'état de préparation opérationnelle;

8. État de préparation opérationnelle/mise en œuvre de la solution

La date d'entrée en fonction de la solution dans le cadre du projet pilote est le 31 mars 2019, à un ensemble identifié d'utilisateurs. À la fin de l'étape du projet pilote, l'entrepreneur doit confirmer l'état de préparation opérationnelle avant de commencer la mise en œuvre progressive de la solution. La mise en œuvre progressive introduira la solution aux utilisateurs restants à l'aide d'une distribution échelonnée entre les mois de juin et septembre 2019.

L'entrepreneur doit :

(a) terminer toutes les activités d'essais;
(b) rendre compte de la réussite des essais en présentant des cas d'essai pour les essais du système (de bout en bout), les essais d'acceptation par les utilisateurs et les essais de rendement;
(c) achever toutes les formations des ressources opérationnelles et techniques comme prévu;
(d) consigner par écrit les commentaires formulés par les participants concernant l'efficacité de la formation;
(e) évaluer la réussite de la formation et en faire rapport;
(f) fournir du matériel de formation, comme une base de connaissances accessible au gouvernement du Canada, des procédures d'utilisation normalisées de bout en bout axées sur le processus, le contenu des modules de formation aux fins de redistribution, des documents de référence, des spécifications fonctionnelles;
(g) relever et consigner par écrit les défauts du système qui n'ont pas encore été résolus;
(h) relever et consigner par écrit les lacunes de la solution;
(i) terminer toutes les activités de communication;
(j) fournir un plan de soutien en service qui prévoit le transfert de connaissances pour les activités;
(k) franchir le point de contrôle 3 du processus d'évaluation et d'autorisation de sécurité;
(l) lancer l'étape du projet pilote;
(m) lancer la mise en œuvre progressive de la solution après la réussite du projet pilote;
(n) mettre à jour le registre des risques et le registre des problèmes;
(o) mettre à jour le calendrier détaillé du projet.

9. Stabilisation et transition de sortie

Au cours de cette période de neuf (9) mois après le lancement de la solution, l'entrepreneur doit continuer d'assurer un soutien dans tous les domaines liés à la solution décrits à l'ANNEXE A, dont la formation, les communications, la

gestion du changement et la correction des défauts. En outre, l'entrepreneur doit assurer une transition harmonieuse des activités de soutien à SPAC pendant cette étape.

L'entrepreneur doit :

(a) fournir un rapport de clôture de projet :
- évaluation du rendement du projet;
- détermination des leçons apprises;
- confirmation que les activités contractuelles essentielles et que les autres activités de clôture du projet ont été menées à bien;
- questions en suspens;
- transfert des biens, des produits livrables et des fonctions administratives en cours.
    - Mesure des avantages/résultats après la mise en œuvre du projet (IRC).

(b) fournir un document rendant compte des enseignements tirés;
(c) effectuer le transfert des connaissances;
(d) fournir des guides de conception portant sur la solution;
(e) fournir toute la documentation concernant la formation, les communications, les processus opérationnels, la gestion du changement et les essais;
(f) fournir des recommandations futures consignées par écrit.

APPENDICE 3 DE L'ANNEXE A - APERÇU DES COMPTES D'UTILISATEURS

APPENDICE 3 DE L'ANNEXE A : APERÇU DES COMPTES D'UTILISATEURS

La présente annexe offre une description détaillée des principaux types de comptes d'utilisateurs pour la solution décrite à l'ANNEXE A.

1. UTILISATEURS EXTERNES

Les clients et partenaires du Secteur de la sécurité industrielle (SSI) qui sont décrits ci-après comme des utilisateurs externes pourront accéder aux services du SSI par l'intermédiaire du service public Web vertical et frontal de la solution.

1.1 Agent de sécurité d'entreprise (ASE)

Un ASE est un citoyen canadien ou un résident permanent employé par une organisation du secteur privé qui est inscrit au Programme de sécurité des contrats (PSC). L'ASE surveille le profil de sécurité de l'organisation, s'occupe des questions de sécurité et rend des comptes au PSC et au cadre supérieur clé désigné de l'organisation sur tout ce qui a trait à la sécurité industrielle. L'ASE est le point de contact avec le PSC au sein de l'organisation. Les comptes des ASE sont créés par le SSI. Les ASE peuvent demander la création de comptes pour des demandeurs ou d'autres ASE.

Service	Actions permises
Généralités	1) Mise à jour des justificatifs d'identité; 2) Mise à jour du profil et des préférences du compte; 3) Accès aux lignes directrices et aux formulaires; 4) Réception d'avis généraux du PSC; 5) Envoi d'avis au PSC; 6) Signature numérique/consentement électronique; 7) Production de rapports; 8) Consultation et établissement du calendrier des événements.
Inscription au PSC	1) Présentation de demandes de services relatives à l'inscription ou au renouvellement de l'inscription de l'organisation au PSC (p. ex. vérification d'organisation désignée (VOD), attestation de sécurité d'installation (ASI), autorisation de détenir des renseignements (ADR), autorisation de déchiquetage, autorisation de stockage de masse et sécurité de la technologie de l'information (TI); 2) Soumission de pièces justificatives (selon les exigences du PSC); 3) Réception d'avis particuliers du PSC; 4) Envoi d'avis particuliers au PSC; 5) Accès à des documents particuliers publiés par le PSC; 6) Suivi de l'état d'avancement des demandes de services relatives à l'inscription ou au renouvellement d'une inscription. 7) Recherche et consultation d'anciennes demandes de services terminées.
Filtrage de sécurité du personnel	1) Demande de création de comptes pour les demandeurs; 2) Demande de création de comptes d'ASE; 3) Présentation de demandes de services de filtrage de sécurité du personnel (nouvelle attestation, mise à jour, reclassement, transfert, enquêtes successives, réactivation et annulation); 4) Remplir les demandes de filtrage de sécurité pour soi et pour le compte de demandeurs; 5) Suivi de l'état d'avancement des demandes de services de filtrage de sécurité du personnel;

	6) Envoi d'avis particuliers au PSC et réception de tels avis du PSC; 7) Envoi aux demandeurs des avis particuliers reçus du PSC; 8) Consultation, élimination ou soumission des pièces justificatives des demandeurs envoyées au PSC; 9) Accès à des documents du PSC (attestations d'initiation, etc.); 10) Consultation d'anciennes demandes de filtrage de sécurité du personnel.
Sous-traitance	1) Achèvement, mise à jour et soumission de listes de vérification des exigences relatives à la sécurité (LVERS); 2) Achèvement, mise à jour et soumission de demandes d'enquête de sécurité sur une organisation du secteur privé; 3) Soumission de pièces justificatives (selon les exigences du PSC); 4) Accès à des documents particuliers publiés par le PSC (p. ex. des clauses de sécurité, les attestations de sécurité de l'organisation du sous-traitant et les attestations individuelles, etc.); 5) Réception d'avis particuliers du PSC; 6) Envoi d'avis particuliers au PSC; 7) Suivi de l'état d'avancement des demandes de services; 8) Consultation d'anciennes demandes de services (terminées).
Demande de visite	1) Présentation de demandes de services pour les demandes de visite; 2) Soumission des modifications (renouvellement, ajouts, suppressions) apportées aux demandes de services visant les demandes de visite. 3) Soumission de pièces justificatives (selon les exigences du PSC); 4) Accès à des documents du PSC (p. ex. formulaire de demande de permis de visite, lettre de renvoi, etc.) 5) Réception d'avis particuliers du PSC; 6) Envoi d'avis particuliers au PSC; 7) Suivi de l'état d'avancement des demandes de services visant les demandes de visite; 8) Recherche ou consultation d'anciennes demandes de visite (terminées).
Transfert de documents	1) Envoi d'un avis relatif au transfert de documents; 2) Soumission de pièces justificatives (selon les exigences du PSC); 3) Réception d'avis particuliers du PSC; 4) Accès à des documents particuliers publiés par le PSC; 5) Suivi de l'état d'avancement des demandes de services relatives au transfert de documents; 6) Consultation et recherche de données antérieures sur le transfert de documents.
Signalement des infractions à la sécurité	1) Envoi au PSC d'un avis signalant une infraction à la sécurité; 2) Soumission de pièces justificatives (selon les exigences du PSC); 3) Réception d'avis particuliers du PSC; 4) Accès à des documents particuliers publiés par le PSC;

1.2 Agent de sécurité du GC

L'agent de sécurité du gouvernement du Canada (GC) est un agent de sécurité d'une organisation gouvernementale qui collabore avec le Secteur de la sécurité industrielle. Cet agent de sécurité est le point de contact avec le PSC. Les comptes des agents de sécurité du GC sont créés par le SSI. Les agents de sécurité du GC peuvent demander la création de comptes d'utilisateur pour des demandeurs et d'autres agents de sécurité du GC. Avant de demander la création de comptes pour des demandeurs ou des ASE, le demandeur doit vérifier leur identité et fournir au PSC les renseignements d'identification de l'utilisateur nécessaires à la création du compte.

Service	Actions permises
Généralités	1) Mise à jour du profil et des préférences du compte; 2) Mise à jour des justificatifs d'identité; 3) Accès aux lignes directrices et aux formulaires; 4) Réception d'avis généraux du PSC; 5) Envoi d'avis au PSC; 6) Signature numérique/consentement électronique; 7) Production de rapports; 8) Consultation et établissement du calendrier des événements.
Parrainer une organisation	1) Présentation de demandes de services d'enquête de sécurité sur une organisation du secteur privé (ESOSP); 2) Soumission de pièces justificatives (selon les exigences du PSC); 3) Suivi de l'état d'avancement des demandes de services relatives à l'inscription; 4) Réception d'avis particuliers du PSC; 5) Envoi d'avis particuliers au PSC; 6) Accès à des documents particuliers publiés par le PSC; 7) Recherche d'anciennes demandes de services de parrainage (terminées).
Filtrage de sécurité du personnel	1) Demande de création ou de suppression de comptes de demandeurs; 2) Envoi d'avis particuliers au demandeur; 3) Réception d'avis particuliers du demandeur; 4) Consultation, annulation et soumission des demandes de filtrage de sécurité et des pièces justificatives dans le système de TI de l'organisation de l'agent de sécurité du GC;
Demande de visite	1) Présentation de demandes de services pour les demandes de visite; 2) Soumission des modifications (renouvellement, ajouts, suppressions) apportées aux demandes de services visant les demandes de visite. 3) Soumission de pièces justificatives (selon les exigences du PSC); 4) Accès à des documents du PSC (p. ex. formulaire de demande de permis de visite, lettre de renvoi, etc.) 5) Réception d'avis particuliers du PSC; 6) Envoi d'avis particuliers au PSC; 7) Suivi de l'état d'avancement des demandes de services visant les demandes de visite; 8) Recherche ou consultation d'anciennes demandes de visite (terminées).

1.3 Demandeur

Le demandeur est un employé d'une organisation du secteur privé inscrite au PSC ou un employé d'un organisme du GC. La création du compte du demandeur est amorcée par un ASE ou un agent de sécurité du GC et achevée par le SSI.

Service	Actions permises
Généralités	1) Mise à jour des justificatifs d'identité; 2) Mise à jour des préférences du compte; 3) Accès aux lignes directrices et aux formulaires; 4) Réception d'avis généraux du PSC; 5) Signature numérique/consentement électronique;
Filtrage de sécurité du personnel	1) Présentation des demandes d'attestation de sécurité du personnel en ligne; 2) Soumission de pièces justificatives (au besoin); 3) Réception d'avis particuliers de l'ASE ou de l'agent de sécurité du GC; 4) Accès à des documents particuliers publiés par l'ASE ou l'agent de sécurité du GC; 5) Envoi d'avis particuliers à l'ASE ou à l'agent de sécurité du GC;

	6) Suivi de l'état d'avancement des demandes de services; 7) Consultation d'anciennes demandes de filtrage de sécurité terminées.

1.4 Agent de sécurité étranger

L'agent de sécurité étranger est un administrateur national de la sécurité ou un administrateur désigné de la sécurité d'un autre pays. Les comptes des agents de sécurité étrangers sont créés par le SSI.

Service	Actions permises
Généralités	1) Accès aux lignes directrices et aux formulaires; 2) Mise à jour du profil et des préférences du compte; 3) Mise à jour des justificatifs d'identité; 4) Réception d'avis généraux du PSC; 5) Envoi d'avis au PSC; 6) Signature numérique/consentement électronique; 7) Production de rapports; 8) Consultation et établissement du calendrier des événements.
Demande de visite	1) Présentation de demandes de services pour les demandes de visite; 2) Soumission des modifications (renouvellement, ajouts, suppressions) apportées aux demandes de services visant les demandes de visite; 3) Soumission de pièces justificatives (selon les exigences du PSC); 4) Accès à des documents du PSC (p. ex. formulaire de demande de permis de visite, lettre de renvoi, etc.) 5) Réception d'avis particuliers du PSC; 6) Envoi d'avis particuliers au PSC; 7) Suivi de l'état d'avancement des demandes de services visant les demandes de visite; 8) Recherche ou consultation d'anciennes demandes de visite (terminées).
Parrainer une organisation	1) Présentation de demandes de services d'enquête de sécurité sur une organisation du secteur privé (ESOSP); 2) Soumission de pièces justificatives (selon les exigences du PSC); 3) Suivi de l'état d'avancement des demandes de services relatives à l'inscription; 4) Réception d'avis particuliers du PSC; 5) Envoi d'avis particuliers au PSC; 6) Accès à des documents particuliers publiés par le PSC; 7) Recherche d'anciennes demandes de services de parrainage terminées.

1.5 Agent d'approvisionnement du GC

Un agent d'approvisionnement du GC est un agent qui effectue des achats spécialisés préalables de biens et de services ou un gestionnaire de projet du GC chargé d'un projet pour lequel les organisations du secteur privé ont fait une soumission ou compte en faire une. Les comptes des agents d'approvisionnement du GC sont créés par le SSI.

Service	Actions permises
Généralités	1) Mise à jour du profil et des préférences du compte; 2) Mise à jour des justificatifs d'identité; 3) Accès aux lignes directrices et aux formulaires; 4) Réception d'avis généraux du PSC; 5) Envoi d'avis au PSC; 6) Signature numérique/consentement électronique; 7) Production de rapports; 8) Consultation et établissement du calendrier des événements.

Parrainer une organisation	1) Présentation de demandes de services d'enquête de sécurité sur une organisation du secteur privé (ESOSP); 2) Soumission de pièces justificatives (selon les exigences du PSC); 3) Suivi de l'état d'avancement des demandes de services relatives à l'inscription; 4) Réception d'avis particuliers du PSC; 5) Envoi d'avis particuliers au PSC; 6) Accès à des documents particuliers publiés par le PSC; 7) Recherche d'anciennes demandes de services de parrainage (terminées).
Garantie contractuelle	1) Achèvement et soumission des LVERS; 2) Consultation et mise à jour des LVERS; 3) Soumission des renseignements sur le contrat; 4) Mise à jour de l'information sur le contrat (modifications); 5) Soumission de pièces justificatives (au besoin); 6) Accès à des documents particuliers publiés par le PSC (p. ex., clauses de sécurité); 7) Réception d'avis particuliers du PSC; 8) Envoi d'avis particuliers au PSC; 9) Suivi de l'état d'avancement des demandes de services; 10) Consultation d'anciennes demandes de services (terminées).

1.6 Personne autorisée

Une personne autorisée est un citoyen canadien ou un résident permanent qui habite normalement au Canada qui fait des affaires au Canada ou qui est le représentant d'une entreprise qui cherche à obtenir ou maintient en vigueur une inscription au Programme des marchandises contrôlées (PMC). Le compte de la personne autorisée est géré par le SSI. Les personnes autorisées peuvent amorcer la création des comptes des représentants désignés.

Service	Actions permises
Généralités	1) Mise à jour des justificatifs d'identité; 2) Mise à jour du profil et des préférences du compte; 3) Accès aux lignes directrices et aux formulaires; 4) Réception d'avis généraux du PMC; 5) Envoi d'avis au PMC; 6) Signature numérique/consentement électronique; 7) Production de rapports; 8) Consultation et établissement du calendrier des événements.
Inscription	1) Procéder à l'inscription au PMC et tenir l'inscription à jour; 2) Soumission de pièces justificatives (p. ex., demande d'évaluation de sécurité, etc.); 3) Réception d'avis particuliers du PMC; 4) Envoi d'avis particuliers au PMC; 5) Accès à des documents particuliers publiés par le PMC (p. ex. copie du certificat d'inscription, etc.); 6) Suivi de l'état d'avancement des demandes de services relatives à l'inscription ou au renouvellement; 7) Recherche et consultation d'anciennes demandes de services terminées.
Nomination d'un représentant désigné	1) Demande de création de comptes de représentants désignés; 2) Soumission d'une demande d'approbation de la nomination du représentant désigné au PMC; 3) Soumission de pièces justificatives (au besoin); 4) Réception d'avis particuliers du PMC;

	5) Envoi d'avis particuliers au PMC; 6) Accès à des documents particuliers publiés par le PMC (p. ex., lettre d'acceptation, copie du certificat du Programme de certification des représentants désignés, etc.); 7) Suivi de l'état d'avancement des demandes de services relatives à l'inscription et à l'approbation de la nomination du représentant désigné; 8) Recherche et consultation d'anciennes demandes de services.
Signalement des infractions à la sécurité	1) Présentation d'un rapport d'atteinte à la sécurité; 2) Soumission de pièces justificatives (selon les exigences du PMC); 3) Réception d'avis particuliers du PMC; 4) Envoi d'avis particuliers au PMC; 5) Accès à des documents particuliers publiés par le PMC;

1.7 Représentant désigné (RD)

Un représentant désigné (RD) est un citoyen canadien ou un résident permanent qui habite normalement au Canada et qui : 1) a été employé par une organisation inscrite au PMC; 2) a été nommé par une personne autorisée du PMC; 3) a été autorisé par le PMC et 4) a réussi le Programme de certification des représentants désignés du PMC. Le RD est le point de contact avec le PMC. La création du compte du RD est amorcée par une personne autorisée et achevée par le SSI.

Service	Actions permises
Généralités	1) Mise à jour des justificatifs d'identité; 2) Mise à jour du profil et des préférences du compte; 3) Accès aux lignes directrices et aux formulaires; 4) Réception d'avis généraux du PMC; 5) Envoi d'avis au PMC; 6) Signature numérique/consentement électronique; 7) Production de rapports; 8) Consultation et établissement du calendrier des événements.
Exemptions d'inscription au PMC;	1) Présentation d'une demande d'exemption d'inscription (visiteur et travailleur temporaire); 2) Soumission de pièces justificatives (p. ex., demande d'évaluation de sécurité, etc.) 3) Réception d'avis particuliers du PMC; 4) Envoi d'avis particuliers au PMC; 5) Accès à des documents particuliers publiés par le PMC; 6) Suivi de l'état d'avancement des demandes de services relatives à l'inscription et au renouvellement; 7) Recherche et consultation d'anciennes demandes de services terminées.
Renvois au PMC	1) Demande d'aide auprès du PMC pour déterminer le statut de l'employé; 2) Soumission de pièces justificatives (p. ex. demande d'évaluation de sécurité, preuve de citoyenneté, vérification nominale du casier judiciaire, etc.) 3) Réception d'avis particuliers du PMC; 4) Envoi d'avis particuliers au PMC; 5) Accès à des documents particuliers publiés par le PMC; 6) Suivi de l'état d'avancement des demandes de services relatives aux renvois; 7) Recherche et consultation d'anciennes demandes de services terminées relatives aux renvois.

Signalement des infractions à la sécurité	1) Présentation d'un rapport d'atteinte à la sécurité; 2) Soumission de pièces justificatives (selon les exigences du PMC); 3) Réception d'avis particuliers du PMC; 4) Envoi d'avis particuliers au PMC; 5) Accès à des documents particuliers publiés par le PMC; 6) Suivi de l'état d'avancement des demandes de services relatives à l'inscription et au renouvellement.

2. UTILISATEURS INTERNES

Un utilisateur interne est un employé du Secteur de la sécurité industrielle responsable du traitement des demandes de service à l'appui du PSC et du PMC. Les comptes des utilisateurs internes ne permettent que l'accès à l'application de traitement des services. Le compte des utilisateurs internes du SSI est créé par l'agent de sécurité des systèmes d'information du SSI. Le niveau et les privilèges d'accès des utilisateurs internes du SSI doivent concorder avec leur niveau d'autorisation et leurs besoins opérationnels.

Voici des exemples des rôles et des responsabilités génériques ainsi que des niveaux et des privilèges d'accès des utilisateurs internes du SSI.

2.1 Commis

Le rôle du commis se limite à des tâches de traitement ou de modification. La principale fonction du commis consiste à effectuer le triage des demandes de service et à faciliter l'acheminement des dossiers de cas à des fins de traitement.

Fonction	Actions permises
Généralités	1) Chercher des cas et des renseignements contenus dans des cas. 2) Consulter des cas et des renseignements contenus dans des cas.
Traitement	1) Traiter les demandes de service dans une mesure restreinte. 2) Lancer des contrôles de sécurité auprès des partenaires. 3) Apporter des modifications aux demandes de service dans une mesure restreinte (p. ex. modification de la cote de priorité des demandes de service; aucune modification aux données soumises avec la demande de service). 4) Saisir les données relatives au traitement des demandes de service (p. ex. justification ou raison des décisions prises ou lecture de codes à barres pour consigner une demande de service soumise). 5) Assigner des dossiers de cas à des fins de traitement complémentaire. 6) Consigner des notes aux cas. 7) Joindre des pièces de différents formats aux dossiers de cas. 8) Fermer des dossiers de cas.
Avis/ Correspondance	1) Générer et envoyer des avis. 2) Générer et envoyer la correspondance. 3) Joindre des avis et de la correspondance à des dossiers de cas. 4) Régler à l'interne des avis servant de rappel pour les activités de suivi.
Rapports	1) Générer les rapports préétablis qui sont disponibles.

2.2 Analyste

Le rôle de l'analyste consiste à traiter les demandes de service. L'analyste doit notamment assumer des fonctions opérationnelles comme celles des analystes des inscriptions, des inspecteurs de la conformité, des enquêteurs, des analystes des centres d'appels, des contrôleurs de la qualité, etc.

Fonction	Actions permises
Généralités	1) Chercher des cas et des renseignements contenus dans des cas. 2) Consulter des cas et des renseignements contenus dans des cas.
Traitement	1) Traiter au complet les demandes de service. 2) Lancer des contrôles de sécurité auprès des partenaires. 3) Lancer des sous-processus internes (comme une demande d'inspection de conformité). 4) Apporter des modifications aux demandes de service dans une mesure restreinte (p. ex. modification de la cote de priorité des demandes de service; aucune modification aux données soumises avec la demande de service). 5) Saisir les données relatives au traitement des demandes de service (p. ex. justification ou raison des décisions prises ou des rapports d'inspection/d'enquête ou lecture de codes à barres pour consigner une demande de service soumise). 6) Ouvrir des dossiers de cas qui peuvent être liés ou non aux cas existants. 7) Assigner des dossiers de cas à des fins de traitement complémentaire. 8) Consigner des notes aux cas. 9) Créer et gérer les activités planifiées (p. ex. les inspecteurs créent des séries d'inspections à l'intérieur d'une zone géographique pour tirer le maximum des frais de déplacement). 10) Joindre des pièces de différents formats aux dossiers de cas. 11) Fermer des dossiers de cas.
Avis/ Correspondance	1) Générer, modifier et envoyer des avis. 2) Générer, modifier et envoyer la correspondance. 3) Joindre des avis et de la correspondance à des dossiers de cas. 4) Régler à l'interne des avis servant de rappel pour les activités de suivi.
Rapports	1) Générer les rapports préétablis qui sont disponibles.
Approbations	1) Accorder les approbations nécessaires (p. ex. le coordonnateur des voyages de conformité du PMC approuve les demandes de voyage soumises avant l'étape des préparatifs de voyage).

2.3 Analyste principal

L'analyste principal exécute les mêmes actions que l'analyste, mais possède davantage de privilèges pour ce qui est des activités de tenue. L'analyste principal est habituellement chef d'équipe ou chef de section.

Fonction	Actions permises
Généralités	1) Chercher des cas et des renseignements contenus dans des cas. 2) Consulter des cas et des renseignements contenus dans des cas.
Traitement	1) Traiter au complet les demandes de service. 2) Lancer des contrôles de sécurité auprès des partenaires. 3) Lancer des sous-processus internes (comme une demande d'inspection de conformité).

	4) Apporter des modifications aux demandes de service (p. ex. modification de la cote de priorité des demandes de service; aucune modification aux données soumises avec la demande de service). 5) Modifier l'information utilisée pour traiter la demande de service; aucune modification aux données soumises avec la demande de service. 6) Saisir les données relatives au traitement des demandes de service (p. ex. justification ou raison des décisions prises ou des rapports d'inspection/d'enquête ou lecture de codes à barres pour consigner une demande de service soumise). 7) Ouvrir des dossiers de cas qui peuvent être liés ou non aux cas existants. 8) Assigner des dossiers de cas à des fins de traitement complémentaire. 9) Consigner des notes aux cas. 10) Modifier les notes déjà consignées dans des cas. 11) Créer et gérer les activités planifiées (p. ex. les inspecteurs créent des séries d'inspections à l'intérieur d'une zone géographique pour tirer le maximum des frais de déplacement). 12) Joindre des pièces de différents formats aux dossiers de cas. 13) Gérer les pièces justificatives et les autres pièces jointes aux dossiers de cas. 14) Fermer des dossiers de cas.
Avis/ Correspondance	1) Générer, modifier et envoyer des avis. 2) Modifier les modèles d'avis. 3) Générer, modifier et envoyer la correspondance. 4) Modifier les modèles de correspondance. 5) Joindre des avis et de la correspondance à des dossiers de cas. 6) Régler à l'interne des avis servant de rappel pour les activités de suivi pour lui-même et pour d'autres analystes.
Rapports	1) Générer les rapports préétablis qui sont disponibles.
Tenue	1) Supprimer.
Approbations	1) Accorder les approbations nécessaires (p. ex. l'analyste principal du PMC fera passer l'état des sites inscrits à « actif » pour les inscriptions au PMC avant d'approuver la demande d'inscription d'une organisation). 2) Accorder les approbations nécessaires et apposer sa signature au besoin pour terminer le traitement d'une demande de service (p. ex. l'analyste principal du PSC approuve et signe la lettre d'admissibilité une fois la demande d'inscription d'une organisation approuvée).

2.4 Gestionnaire/directeur

Le rôle du gestionnaire en est surtout un de lecture seule à des fins d'information; le gestionnaire peut accorder des approbations au besoin.

Fonction	Actions permises
Généralités	1) Chercher des cas et des renseignements contenus dans des cas. 2) Consulter des cas et des renseignements contenus dans des cas.
Traitement	1) Assigner des dossiers de cas à des fins de traitement complémentaire. 2) Consigner des notes aux cas. 3) Modifier les notes déjà consignées dans des cas. 4) Joindre des pièces de différents formats aux dossiers de cas. 5) Gérer les pièces justificatives et les autres pièces jointes aux dossiers de cas.

	6) Apporter des modifications aux demandes de service (p. ex. modification de la cote de priorité des demandes de service; aucune modification aux données soumises avec la demande de service). 7) Saisir les données relatives au traitement des demandes de service (p. ex. justification ou raison des décisions prises ou des rapports d'inspection/d'enquête ou lecture de codes à barres pour consigner une demande de service soumise).
Avis/ Correspondance	1) Générer, modifier et envoyer la correspondance.
Rapports	1) Générer les rapports préétablis qui sont disponibles.
Approbations	1) Accorder les approbations nécessaires (p. ex. le directeur du PSC doit approuver les suspensions). 2) Accorder les approbations nécessaires et apposer sa signature au besoin pour terminer le traitement d'une demande de service (p. ex. le gestionnaire de la conformité passera en revue les rapports d'inspection à des fins d'approbation écrite dans le cadre du processus d'approbation de la demande d'inscription d'une organisation).

2.5 Utilisateur ayant accès pour lecture seulement

L'utilisateur ayant accès pour lecture seulement peut chercher et visualiser des données, mais ne peut apporter aucune modification ni générer d'avis, de correspondance ou de rapports.

Fonction	Actions permises
Généralités	1) Chercher des cas et des renseignements contenus dans des cas. 2) Consulter des cas et des renseignements contenus dans des cas.

2.6 Administrateur de système

L'administrateur de système assume un rôle de lecture seulement dans le seul but d'effectuer les travaux de maintenance opérationnelle au niveau du système exigeant un accès contrôlé. Les activités exécutées par l'administrateur de système exigent une bonne connaissance de la solution et des fonctions opérationnelles nécessaires pour exécuter de telles actions.

Fonction	Actions permises
Généralités	1) Chercher des cas et des renseignements contenus dans des cas. 2) Consulter des cas et des renseignements contenus dans des cas.
Tenue	1) Créer et modifier des modèles d'avis. 2) Créer et modifier des modèles de correspondance. 3) Créer, désactiver, supprimer et modifier des comptes d'utilisateurs (p. ex. renseignements de base sur les comptes des utilisateurs). 4) Ajouter ou supprimer des capacités ou des rôles disponibles pour les comptes d'utilisateurs. 5) Ajouter, modifier, supprimer ou désactiver les capacités qui sont disponibles et qui peuvent être assignées à un rôle d'utilisateur. 6) Ajouter, modifier, supprimer ou désactiver les règles/processus opérationnels existants qui sont utilisés par la solution dans son ensemble (p. ex. tant le portail Web destiné à l'extérieur que l'application de traitement interne) pour la mise en œuvre des politiques et des règles/processus opérationnels à venir. 7) Ajouter, modifier, supprimer ou désactiver les flux de travaux dans la solution.

	8) Tenir à jour les formulaires opérationnels pour le traitement des cas (p. ex. ajouter de nouveaux champs de données aux formulaires pour consigner de l'information supplémentaire ou désactiver des champs de données existants qui ne sont plus requis). 9) Modifier les formulaires destinés à l'extérieur et les publier sur le portail Web des solutions. 10) Ajouter, modifier, supprimer ou désactiver la solution, en tout ou en partie. 11) Conserver les contrôles et les permissions d'accès au niveau des champs pour le rôle d'utilisateur. 12) Mettre à jour un environnement de mise à l'essai à l'aide d'une copie de la solution provenant de la production (demande seulement; aucune donnée). 13) Être en mesure d'activer/de désactiver un lien affiché sur le portail Web des solutions (Exigence opérationnelle APP-OPS.22). 14) Conserver l'accès aux différents environnements utilisés pour soutenir la solution.
Tenue des rapports	1) Générer les rapports préétablis qui sont disponibles. 2) Ajouter, modifier, supprimer ou désactiver les rapports qui sont disponibles dans la solution. 3) Ajouter, modifier, supprimer ou désactiver les critères de sélection associés à un rapport. 4) Ajouter, modifier, supprimer ou désactiver les rapports qui peuvent être consultés en fonction du rôle de l'utilisateur et/ou du compte de l'utilisateur. 5) Ajouter, modifier, supprimer ou désactiver les requêtes de rapport personnalisé, qui peuvent mener ou non à un nouveau rapport disponible dans la solution.
Approbations	1) Approuver les demandes de compte d'utilisateur.

APPENDICE 4 DE L'ANNEXE A - EXIGENCES PRÉVUES PAR LES LOIS, LES RÈGLEMENTS ET LES POLITIQUES

APPENDICE 4 DE L'ANNEXE A – EXIGENCES PRÉVUES PAR LES LOIS, LES RÈGLEMENTS ET LES POLITIQUES

Le présent appendice présente les exigences prévues par les lois, les règlements et les politiques ainsi que les références connexes qui s'appliquent aux travaux décrits à l'*ANNEXE A – Énoncé des travaux (ET)*. L'entrepreneur et la solution doivent se conformer directement à l'ensemble des politiques, des directives et des lignes directrices fédérales, y compris, sans toutefois s'y limiter, celles compris dans cette APPENDICE. L'autorité de projet informera l'entrepreneur des lois, des règlements, des directives, des normes et des lignes directrices fédéraux ou législatifs nouveaux ou modifiés qui ont un impact sur le projet.

1. INTRODUCTION

Les lois, les règlements, les politiques, les directives, les normes et les lignes directrices donnent d'autres renseignements utiles permettant de déterminer les exigences liées à la conformité de la solution et de la prestation de services au GC, ainsi que la portée et la complexité du déroulement des activités et des exigences fonctionnelles qui doivent être mises en œuvre.

Même si l'emplacement actuel de la dernière version de chaque document électronique est indiqué, tous les documents peuvent faire l'objet de modifications et la solution doit favoriser la conformité continue du GC à toutes les exigences prévues par les lois, les règlements et les politiques.

2. LOIS ET RÈGLEMENTS

Les services offerts par l'intermédiaire de la solution doivent faciliter le respect de l'ensemble des politiques, directives et lignes directrices du gouvernement du Canada, y compris, sans toutefois s'y limiter, celles qui suivent :

Loi sur la gestion des finances publiques	http://laws-lois.justice.gc.ca/fra/lois/f-11/
Loi sur l'accès à l'information	http://laws-lois.justice.gc.ca/fra/lois/a-1/
Loi sur la protection des renseignements personnels	http://laws-lois.justice.gc.ca/fra/lois/p-21/
Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)	http://laws-lois.justice.gc.ca/fra/lois/p-8.6/
Loi sur la Bibliothèque et les Archives du Canada	http://laws-lois.justice.gc.ca/fra/lois/l-7.7/
Loi sur les langues officielles	http://laws-lois.justice.gc.ca/fra/lois/o-3.01/
Loi sur la production de défense	http://laws-lois.justice.gc.ca/fra/lois/d-1/
Loi sur les forces étrangères présentes au Canada.	http://lois-laws.justice.gc.ca/fra/lois/V-2/
Code criminel	http://laws-lois.justice.gc.ca/fra/lois/c-46/
Loi sur la preuve au Canada	http://laws-lois.justice.gc.ca/fra/lois/C-5/
Loi sur le casier judiciaire;	http://laws-lois.justice.gc.ca/fra/lois/c-47/
Loi sur les licences d'exportation et d'importation	http://laws-lois.justice.gc.ca/fra/lois/E-19/
Règlement sur les marchandises contrôlées	http://laws-lois.justice.gc.ca/fra/reglements/DORS-2001-32/
Règlement sur les signatures électroniques sécurisées	http://laws-lois.justice.gc.ca/fra/reglements/DORS-2005-30/page-1.html

Toutes les autres lois fédérales, y compris celles qui ne figurent pas sur la liste ci-dessous, se trouvent dans leur intégralité sur le site Web du ministère de la Justice à l'adresse *www.justice.gc.ca*.

3. POLITIQUES, DIRECTIVES, NORMES ET LIGNES DIRECTRICES

L'entrepreneur et la solution doivent se conformer directement à l'ensemble des politiques, des directives et des lignes directrices fédérales, y compris, sans toutefois s'y limiter, celles qui suivent :

Cadre stratégique pour l'information et la technologie	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12452
Politique sur la gestion de l'information	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12742
Politique sur la gestion des technologies de l'information	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12755
Politique sur la protection de la vie privée	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510
Politique sur l'accès à l'information	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12453
Politique sur la sécurité du gouvernement	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578
Directive sur la gestion de la sécurité ministérielle;	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16579
Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328
Norme opérationnelle sur la sécurité matérielle	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329
Norme sur le filtrage de sécurité	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115
Norme de sécurité et de gestion des marchés	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12332
Norme opérationnelle de la Loi sur la protection de l'information.	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12323
Norme de sécurité relative à l'organisation et l'administration	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12333
Politique sur la gestion financière	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32495
Politique sur l'audit interne	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16484
Politique de communication et de coordination de l'image de marque	https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=30683
Directive sur la gestion de l'identité;	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16577
Directive concernant l'administration de la Loi sur l'accès à l'information	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18310
Directive sur la gestion des technologies de l'information	https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=15249
Politique sur l'utilisation acceptable des dispositifs et des réseaux	https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27122

Tous les autres politiques du Conseil du Trésor et les instruments connexes, y compris ceux qui ne figurent pas sur la liste ci-dessous, se trouvent dans leur intégralité sur le site Web du Secrétariat du Conseil du Trésor du Canada (http://www.tbs-sct.gc.ca/pol/index-fra.aspx).

4. POLITIQUES, NORMES ET DIRECTIVES RÉGISSANT LA PRESTATION DE SERVICES EN LIGNE

L'entrepreneur et la solution doivent se conformer directement à l'ensemble des politiques, des directives et des lignes directrices fédérales concernant la prestation de services en ligne, y compris, sans toutefois s'y limiter, celles qui suivent :

Norme sur l'accessibilité Web	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601
Norme sur la facilité d'emploi des sites Web	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=24227
Norme sur l'interopérabilité du Web	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=25875
Norme sur l'optimisation des sites Web et des applications pour appareils mobiles	https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27088
Spécifications techniques relatives à la présence Web et mobile	http://www.tbs-sct.gc.ca/ws-nw/mo-om/ts-st/index-fra.asp
Norme sur la protection de la vie privée et le Web analytique	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26761
Norme sur la gestion du courriel	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27600

Tous les autres instruments de communication Web du Conseil du Trésor, y compris ceux qui ne figurent pas sur la liste ci-dessous, se trouvent dans leur intégralité sur le site Web du Secrétariat du Conseil du Trésor du Canada (http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/index-fra.asp).

5. LIGNES DIRECTRICES SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

L'entrepreneur et la solution doivent suivre les lignes directrices sur la sécurité des technologies de l'information généralement reconnues du gouvernement et du secteur y compris, sans toutefois s'y limiter, celles qui suivent :

La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie (ITSG-33)	https://www.cse-cst.gc.ca/fr/node/265/html/22814
Exigences de sécurité liées aux réseaux locaux sans fil (ITSG-41)	https://www.cse-cst.gc.ca/fr/node/264/html/27578
Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones (ITSG-38)	https://www.cse-cst.gc.ca/fr/node/266/html/25034
Le Guide de travail pour l'évaluation des menaces et des risques (ITSG-04) a été remplacé par la Méthodologie harmonisée d'évaluation des menaces et des risques	https://www.cse-cst.gc.ca/fr/publication/tra-1
Guide sur l'authentification des utilisateurs pour les systèmes TI (ITSG-31)	https://www.cse-cst.gc.ca/fr/node/1842/html/26717
Exigences de base en matière de sécurité pour les zones de sécurité de	https://www.cse-cst.gc.ca/fr/node/268/html/15236

réseau au sein du gouvernement du Canada (ITSG-22)	
Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B	https://www.cse-cst.gc.ca/fr/node/1831/html/26515
Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information	https://www.cse-cst.gc.ca/fr/node/1842/html/26717
Effacement et déclassification des supports d'information électroniques	https://www.cse-cst.gc.ca/fr/node/270/html/10573
PUBLICATIONS SPÉCIALES DU NIST	http://csrc.nist.gov/publications/PubsSPs.html#800

Toutes les lignes directrices du CST, y compris celles qui ne figurent pas sur la liste ci-dessous, se trouvent dans leur intégralité sur la page *Conseils et directives en matière de STI*.
du site Web du CST (https://www.cse-cst.gc.ca/fr/group-groupe/conseil-directives-matiere-sti).

6. PROGRAMME DE SÉCURITÉ DES CONTRATS – FORMULAIRES ET LIGNES DIRECTRICES

L'entrepreneur et la solution doivent se conformer directement à l'ensemble des formulaires et lignes directrices pertinents du Programme de sécurité des contrats, y compris, sans toutefois s'y limiter, ceux qui suivent :

Manuel de la sécurité industrielle	
Manuel de la sécurité industrielle	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/index-fra.html
Enquêtes de sécurité sur le personnel	
Formulaire d'enquête de sécurité sur le personnel (TBS/SCT 330-23)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-23-fra.asp
Formulaire d'autorisation de sécurité (TBS/SCT 330-60)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-60-fra.asp
Certificat d'enquête de sécurité et profil de sécurité (TBS/SCT 330-47)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-47-fra.asp
Liste de vérification des exigences relatives à la sécurité (TBS/SCT 350-103)	http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-fra.asp
Rapport d'incident de sécurité de l'agent de sécurité d'entreprise et l'agent de sécurité d'entreprise remplaçant	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/rapport-incident-report-fra.html
Signalement des incidents de sécurité	http://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/signalement-reporting-fra.html
Formulaire d'attestation de l'agent de sécurité d'entreprise ou de l'agent de sécurité d'entreprise remplaçant	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/attestation-fra.html
Consentement pour la divulgation de renseignements concernant le niveau d'enquête de sécurité et d'autorisation de sécurité	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/cnsntmnt-cnsnt-fra.html
Guide de l'agent de sécurité d'entreprise sur la façon de remplir et présenter les formulaires d'enquête de sécurité sur le personnel	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/index-fra.html

Comment remplir le Formulaire de vérification de sécurité, de consentement et d'autorisation du personnel (SCT/TBS 330-23F)	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/330-23-fra.html
Comment remplir le Formulaire d'autorisation de sécurité (SCT/TBS 330-60F)	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/330-60-fra.html
Comment remplir le Certificat d'enquête de sécurité et profil de sécurité (TBS/SCT 330-47)	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/330-47-fra.html
Sécurité des contrats	
Liste de vérification des exigences relatives à la sécurité *(TBS/SCT 350-103)*	http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-fra.asp
Enquête de sécurité sur les organisations	
Formulaire de demande d'enquête de sécurité sur une organisation du secteur privé	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/esosp-psos-fra.html
Annexe 1-A –Nomination d'un agent général de sécurité d'entreprise ou d'un agent de sécurité d'entreprise Accusé de réception et engagement	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-1a-fra.html
Annexe 1-B – Nomination d'un agent de sécurité d'entreprise remplaçant – Accusé de réception et engagement	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-1b-fra.html
Annexe 3-G – Services publics et Approvisionnement Canada – Accord sur la sécurité	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3g-fra.html
Annexe 3-D – Résolution en vue de l'exemption d'une organisation mère	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3d-fra.html
Annexe 3-E – Certificat de non-divulgation	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3e-fra.html
Annexe 3-F – Résolution du conseil d'administration de l'organisation filiale pour prendre acte de l'exclusion de l'organisation mère et résolution visant à exclure l'organisation mère	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3f-fra.html
Obtention d'une attestation de sécurité pour votre organisation	http://www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/enquete-screening-fra.html
Protection de l'organisation	
Annexe 5-A – Document de demande d'inscription pour l'achat d'équipement	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5a-fra.html
Transport et transmission	
Annexe 5-D, appendice A-1 – Ordre de mission du courrier	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a1-fra.html
Annexe 5-D, appendice A-3 – Déclaration préalable –Services de sécurité et d'information	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a3-fra.html
Appendice A-4 de l'annexe 5-D – Déclaration finale	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a4-fra.html

Annexe 5-C - Normes applicables à la transmission de renseignements et de biens PROTÉGÉS et CLASSIFIÉS	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5c-fra.html
Transfert de renseignements et de biens de nature délicate	http://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/transfert-transfer-fra.html
Visites	
Formulaire de demande de visite	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/visite-visits-fra.html
Approbation des visites de lieux de travail sécurisés	http://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/visite-visit-fra.html

Tous les autres formulaires et lignes directrices du Programme de sécurité des contrats, y compris ceux qui ne figurent pas sur la liste ci-dessous, se trouvent sur le site Web de la Sécurité industrielle (http://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html).

7. PROGRAMME DES MARCHANDISES CONTRÔLÉES – FORMULAIRES ET LIGNES DIRECTRICES

L'entrepreneur et la solution doivent se conformer directement à l'ensemble des formulaires et lignes directrices pertinents du Programme des marchandises contrôlées, y compris, sans toutefois s'y limiter, ceux qui suivent :

Inscription	
Demande d'inscription	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/inscription-registration-fra.html
Demande d'évaluation de sécurité – propriétaire, personne autorisée, représentant désigné, cadre, administrateur, employé	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/des-saa-fra.html
Sommaire de l'évaluation de sécurité par le représentant désigné qui réalise l'évaluation de sécurité d'un employé, d'un administrateur ou d'un cadre	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/ses-sas-fra.html
Lignes directrices sur l'inscription au Programme des marchandises contrôlées	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/inscription-registration-fra.html
Guide de la nouvelle Annexe de la Loi sur la production de défense	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/lpd-dpa-toc-fra.html
Inspections et conformité	
Lignes directrices sur les inspections de conformité du Programme des marchandises contrôlées	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/inspections-fra.html
Liste de vérification préalable à l'inspection	http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/comment-how/liste-checklist-fra.html
Élaborer un plan de sûreté pour les marchandises contrôlées	http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/comment-how/ps-sp-fra.html
Formulaire d'atteinte à la sécurité	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/as-sbr-fra.html
Exemptions d'inscription	
Demande d'exemption pour l'inscription – travailleur temporaire ou étudiant étranger	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/travailleur-worker-fra.html

Demande d'évaluation de sécurité et d'exemption d'inscription pour visiteur	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/visiteurs-visitors-fra.html
Demande d'évaluation de sécurité – travailleur temporaire ou étudiant étranger	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/des-travailleur-saa-worker-fra.html
Représentants désignés	
Formation obligatoire pour les représentants désignés	http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/enregistrement-register/formation-training-fra.html
Lignes directrices sur les représentants désignés	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/rd-directives-do-guidelines-fra.html

Tous les autres formulaires et lignes directrices du Programme des marchandises contrôlées, y compris ceux qui ne figurent pas sur la liste ci-dessous, se trouvent sur le site Web du Programme des marchandises contrôlées (http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/index-fra.html).

APPENDICE 5 DE L'ANNEXE A – GLOSSAIRE DES TERMES

APPENDICE 5 DE L'ANNEXE A – GLOSSAIRE DES TERMES

Le présent appendice fournit une description des principaux termes utilisés dans l'*ANNEXE A – Énoncé des travaux (EDT)*. Il doit être utilisé en conjonction avec l'*appendice 6 de l'ANNEXE A : Sigles et abréviations*.

A

Accès à distance : accès aux systèmes de TI de la SSI au moyen d'un réseau externe (p. ex. l'Internet).

Accès non autorisé : lorsqu'une entité obtient un accès non autorisé à la solution afin de commettre un autre crime comme voler ou détruire des renseignements contenus dans la solution (p. ex. infiltration, atteinte à l'intégrité, piratage, escalade de privilèges et accès/privilège non autorisé).

Accès sécurisé : capacité d'autoriser ou de refuser à un utilisateur l'accès aux ressources de la solution.

Administrateur autorisé : personne dont le rôle consiste à gérer les fonctions avancées du système dans le cadre de la solution, notamment la configuration des règles opérationnelles, les flux de travail, etc.

Administrateur de système : rôle défini pour l'entretien technique, la configuration et le fonctionnement sécurisé de la solution.

Agent de sécurité des systèmes d'information (ASSI) : rôle d'utilisateur privilégié défini et autorisé pour la gestion du contrôle d'accès dans la solution. L'ASSI créée, modifie, désactive et vérifie les comptes d'utilisateur pour les utilisateurs internes et externes.

Agent de sécurité du gouvernement du Canada : agent de sécurité d'une organisation gouvernementale qui collabore avec le Secteur de la sécurité industrielle. Cet agent de sécurité est le point de contact avec le PSC. Aux fins de la solution, l'agent de sécurité du gouvernement du Canada est un utilisateur externe.

Agent de sécurité étranger : agent étranger officiellement désigné comme autorité nationale en matière de sécurité ou comme autorité désignée en matière de sécurité d'un autre pays.

Analyse des causes fondamentales : décrit une vaste gamme d'approches, d'outils et de techniques utilisés pour cerner les causes des problèmes.

Agents du programme PSC/PMC : agents d'enregistrement, agents, de vérification du personnel de sécurité, inspecteurs, enquêteurs, etc.

Analyses : application de formules mathématiques, de statistiques, de demandes, de cubes d'information et d'autres objets de données pour analyser divers aspects de la solution pour le soutien en service.

Aperçu : affichage des données à un moment particulier.

Architecture axée sur le service (AAS) : modèle architectural dans la conception logicielle dont les composantes fournissent des services aux autres composantes par l'entremise d'un protocole de communication, habituellement dans le cadre d'un réseau. Les principes axés sur le service sont indépendants de tout fournisseur, tout produit ou toute technologie.

Architecture des données : composée de modèles, de politiques, de règlements ou de normes selon lesquels on décide des données qui seront recueillies, de la façon dont elles seront sauvegardées, organisées, intégrées et utilisées dans les systèmes de données et les organisations.

Architecture technologique : activités associées à la conception et à l'élaboration de l'infrastructure et de l'application de la TI ainsi qu'aux outils qui appuient le service de TI.

Archivage de fichiers: Suppression d'un enregistrement des données de production de sorte qu'il ne peut plus être consulté ni modifié.

Assistant intelligent : assistant intelligent est une interface utilisateur qui présente une série de fenêtres de dialogue qui guident l'utilisateur lorsqu'il effectue une série de tâches bien précises Les tâches qui sont complexes, peut souvent exécutées ou peu connues peuvent être plus faciles à faire avec un assistant intelligent (p. ex. configuration de l'utilisateur).

Assurance de la qualité : système d'activités dont le but est d'assurer que le contrôle de la qualité est effectué efficacement. Pour un produit ou un service précis, ceci comprend la vérification et l'évaluation des facteurs de qualité qui ont une incidence sur les spécifications, la production, l'inspection et la distribution.

Authentification : processus servant à vérifier les justificatifs de sécurité (p. ex. identité numérique) d'un utilisateur de la solution.

Autorisation de sécurité : processus continu d'obtention et de maintien de la décision de gestion par un représentant organisationnel principal, pour autoriser le fonctionnement d'un système d'information et pour explicitement accepter le risque de se fier sur le système d'information afin d'appuyer les activités opérationnelles basées sur la mise en œuvre d'un ensemble de contrôles de sécurité approuvé et sur les résultats de l'évaluation continue de la sécurité. La solution sera autorisée par le dirigeant principal de l'information de SPAC.

Autres ministères gouvernementaux : tout ministère ou toute agence autre que Services publics et Approvisionnement Canada

B

Base de connaissances : répertoire pour la gestion de connaissances sur le rendement qui permet de recueillir, organiser, extraire et échanger des renseignements actuels et historiques. La base de connaissances fournit l'information, la raison ou la justification pour prendre une décision informée.

C

Capacité d'adaptation : capacité d'un système, d'un réseau ou d'un processus de traiter une charge de travail de façon efficace ou sa capacité d'être enrichi pour répondre à une demande accrue. Cette capacité permet à l'équipement informatique et au programme d'évoluer avec le temps, lesquels n'ont alors pas besoin d'être remplacés. Un réseau évolutif doit pouvoir compter des connexions supplémentaires sans que les transferts de données soient ralentis. Dans chaque cas, l'équipement évolutif peut être enrichi pour répondre aux demandes croissantes. Tous les appareils et logiciels ont des limites, mais l'équipement et les programmes évolutifs offre un avantage à long terme par rapport à ceux qui ne sont pas conçus pour être mis à niveau au fil du temps.

Cas d'utilisation : outil d'analyse qui décrit les tâches qu'un système, qu'une solution ou qu'un service exécute pour un acteur et les objectifs que l'acteur atteindra comme résultat du processus. Le résultat devrait être observable et mesurable et représenter une valeur pour l'acteur.

Centre de données : installation utilisée pour héberger des systèmes informatiques et des composantes connexes, comme des systèmes de télécommunication et de stockage.

Client : dans le contexte de la solution, un utilisateur externe.

Code mobile : Programme (p. ex. script, macro, ou autres instructions portables) qui peut être expédié inchangé à une collection hétérogène de plateformes et exécuté avec une sémantique identique.

Comptes génériques : tout compte qui n'est pas unique. Un compte d'utilisateur est habituellement unique et attribué à un utilisateur précis, tandis qu'un compte générique est utilisé par de nombreux utilisateurs ou processus systémiques.

Confidentialité : divulgation non autorisée de renseignements ou de biens de nature délicate, selon la classification ou la désignation, chacun impliquant un certain préjudice en cas de divulgation non autorisée.

Consommateur : bénéficiaire ultime des services professionnels de l'intégrateur de systèmes.

Contrôle d'accès : contrôles de sécurité permettant d'autoriser ou d'interdire l'accès aux ressources de la solution.

Contrôle de la qualité : gamme d'activités visant à assurer et que la qualité propre du produit ou du service a été obtenue et à vérifier si c'est le cas.

Cryptage : transformation de données intelligibles en une suite de caractères inintelligibles au moyen d'un processus de codage réversible (voir « cryptographie »).

Cryptographie : discipline qui porte sur les principes, les moyens et les méthodes visant à protéger les renseignements ordinaires en les rendant inintelligibles. Il s'agit également de reconvertir les renseignements inintelligibles en renseignements intelligibles (voir « chiffrement »).

Cycle de vie de développement du système : désigne les procédures documentées et mises en œuvre pour guider et contrôler la conception, l'élaboration, l'approbation, l'essai, la documentation, la mise en œuvre, la maintenance et la protection de logiciels de production et d'éléments de données.

Cycle de vie de l'élaboration des logiciels : Le cycle de vie de l'élaboration de logiciels décrit un processus pour la planification, la création, l'essai et l'élaboration d'un système d'information.

D

Délégué : toute personne à qui on a donné l'autorisation d'agir au nom d'un autre utilisateur pour exécuter ou approuver un groupe de tâches définies.

Demandeur : un employé d'une entreprise du secteur privé inscrite au Programme de sécurité des contrats (PSC), ou employé d'un organisme gouvernemental qui collabore avec le PSC relativement aux services de filtrage de sécurité du personnel.

Déni de service : tentative de rendre les ressources d'une machine ou d'un réseau non disponibles aux utilisateurs visés (p. ex. attaque à la bande passante, déni de service distribué, rétrodiffusion, attaque à la consommation des ressources du système, entrave à la communication, perturbation des renseignements sur l'état, interruption de l'acheminement ou liée aux renseignements DNS et mutilation de sites Web).

Données de gestion des SSI : données dérivées de l'exploitation, de l'administration et de la gestion de la solution que l'entrepreneur utilise directement pour ce qui suit :

a) demandes de service;
b) dossiers d'incident (sauf les dossiers d'incidents liés à la sécurité);
c) dossiers sur les biens;
d) dossiers de configuration;
e) renseignements sur la performance du système, la capacité et la planification des ressources;
f) alarmes et événements (sauf les alarmes et les événements qui touchent la sécurité).

Données du SSI : ensemble des données liées à la solution.

Données du système du SSI : les données que l'entrepreneur utilise pour contrôler ou modifier l'exploitation, l'administration et la gestion du SSI comprennent les données sur ce qui suit :

a) incidents de sécurité;
b) gestion de l'information et des événements de sécurité;
c) gestion du périmètre du réseau (p. ex. pare-feu);
d) gestion des intrusions et de la prévention;
e) protection contre les virus, les pourriels et les logiciels malveillants;
f) gestion de l'hyperviseur et des systèmes de la machine virtuelle;
g) gestion du réseau et opérations;
h) fichiers, registres et scripts relatifs à la configuration du système;
i) systèmes d'authentification, d'autorisation et de comptabilité;
j) systèmes disques;
k) service de gestion;
l) prestation de services du service public Web vertical et frontal;
m) systèmes de gestion des ressources et de la capacité;
n) distribution et mise à jour des logiciels et application de correctifs;
o) services d'annuaire.

Données ouvertes : pratique qui rend les données plus disponibles au public pour qu'il puisse être possible de réutiliser les données.

Données sur les utilisateurs du SSI : comprend le compte, les notifications, les affichages personnalisés et les filtres.

Dossier électronique : dossier de médias de stockage électroniques, produit, communiqué, mis à jour ou accédé au moyen d'équipement électronique.

Dossier : renseignement dans tout format créé, reçu et conservé comme preuve, et renseignement par une organisation ou une personne, conformément aux obligations légales ou dans une transaction opérationnelle.

Droit d'accès minimal : principe de sécurité selon lequel les utilisateurs de la solution doivent recevoir le minimum de droits d'accès dont ils ont besoin pour exécuter leur travail sans entraves.

Droits d'accès : façon de contrôler, de réglementer ou de restreindre l'accès au système à un utilisateur en fonction des rôles et des privilèges de ce dernier.

Duplication des cotes et attestations de sécurité : l'attestation de sécurité ou la cote de fiabilité d'un entrepreneur individuel employé par plusieurs organisations enregistrées peuvent être reproduites si les critères suivants sont respectés : la cote et l'attestation sont toujours valides; elles ne doivent pas être mises à jour; l'organisation qui demande la reproduction est enregistrée et en règle dans le Programme de sécurité des contrats.

E

Échange de données informatisées (EDI) : désigne le processus de transfert direct de données d'un système à l'autre.

Entente internationale bilatérale sur la sécurité industrielle : le Programme de sécurité industrielle (PSI) négocie des ententes internationales bilatérales sur la sécurité industrielle comme des arrangements, des protocoles d'entente, etc. avec d'autres pays. Ces instruments portent sur l'échange et la protection des renseignements et des biens protégés et classifiés. À l'échelle internationale, les alliés du Canada reconnaissent la Direction de la sécurité industrielle internationale (DSII) comme l'autorité désignée en matière de sécurité (ADS) industrielle.

Enterprise Service Bus (ESB) : modèle d'architecture logicielle utilisé pour concevoir et mettre en œuvre la communication entre les applications logicielles dans une architecture axée sur les services.

Entrepôt de données : système utilisé pour l'établissement de rapports et l'analyse des données. Les entrepôts de données sont des dépôts centraux de données intégrées provenant de sources diverses. Ils stockent des données actuelles et historiques et servent à créer des rapports d'analyse à l'intention des travailleurs du savoir dans l'ensemble de l'entreprise.

Environnement d'essai de contrôle : équivalent d'un essai d'acceptation par l'utilisateur ou d'un environnement de préproduction.

Étape de réalisation : voir le Système national de gestion de projet (SNGP). L'étape de réalisation de projet vise à transformer les objectifs et les exigences approuvés du projet en critères techniques afin de permettre la conception détaillée et la mise en œuvre complète du produit final. L'équipe de projet élaborera, mettra à l'essai, mettra en œuvre et transférera le produit, le service ou le résultat du projet vers les opérations, et elle achèvera le projet de façon harmonieuse. Les questions en suspens seront acheminées aux responsables opérationnels.

Évaluation de la menace et des risques : processus structuré conçu pour déterminer les risques et fournir des recommandations quant à l'atténuation des risques grâce à l'analyse de système/d'actifs essentiels en matière de service, d'événements/de scénarios posant une menace potentielle et les vulnérabilités connexes.

Évaluation de la sécurité : processus d'évaluation continu du rendement des contrôles de sécurité de la TI durant le cycle de vie des systèmes d'information afin d'établir la mesure dans laquelle les contrôles sont bien mis en œuvre, fonctionnent comme prévu et produisent le résultat souhaité pour répondre aux besoins opérationnels du ministère en matière de sécurité. L'évaluation de la sécurité appuie l'autorisation en donnant une raison d'avoir

confiance dans la sécurité des systèmes d'information. La sécurité de la solution sera évaluée par l'autorité de la TI de SPAC.

Expérience consommateur : qui fournit une expérience de commerce au détail.

F

Fiabilité simple (code de fiabilité simple) : type de vérification de sécurité requise avant qu'un employé puisse avoir accès à des renseignements, des biens ou des lieux de travail qui sont protégés A, B ou C. Elle est valide pendant 10 ans.

Fiabilité : mesures exprimées quant à la capacité d'un produit à fonctionner efficacement au besoin, pendant la période requise, dans l'environnement précisé.

Flux de travail : acheminement de renseignements selon un processus prescrit associé à un produit ou service particulier. Ces processus peuvent être configurés en fonction des commodités, des règles opérationnelles et des étapes connexes (p. ex., collaboration, examen, validation, évaluation de la soumission et approbation).

Formateur : personne responsable de montrer aux utilisateurs comment utiliser la solution.

Formation des formateurs : programme de formation visant à enseigner aux participants comment donner une formation pratique aux utilisateurs de la solution.

G

Gestion de documents : coordination et contrôle du flux (stockage, retrait, traitement, impression, acheminement et distribution) de documents électroniques et papier de façon sécuritaire et efficiente, afin d'assurer qu'ils sont accessibles au personnel autorisé au besoin.

Gestion de la charge de travail : capacité d'attribuer, de planifier et de gérer les tâches et les calendriers pour les utilisateurs, y compris la capacité de désigner des travailleurs pour les secteurs de services, de gérer la disponibilité, de gérer le volume et le type de tâches en fonction des ressources aussi efficacement que possible, et ce, conformément aux objectifs prédéterminés liés aux niveaux de service.

Gestion de processus : ensemble des activités de planification et de surveillance du rendement d'un processus opérationnel. Une organisation établit et maintient un environnement de réseautage digne de confiance en gérant les clés et les certificats au moyen d'une infrastructure à clés publiques.

Gestion des connaissances : processus qui institutionnalise les pratiques exemplaires, le matériel de formation et les politiques organisationnelles à des fins d'accès rapide et facile.

Gestion des correctifs : méthodes et procédures normalisées visant à minimiser l'incidence des problèmes sur la solution.

Gestion des incidents : responsable de la gestion du cycle de vie de tous les incidents informatique affectant les applications et les services de production. La gestion des incidents a pour but de rétablir le service pour le client aussi rapidement que possible plutôt que d'essayer de trouver une solution permanente.

Gestion des justificatifs : collecte, suivi (p. ex. documents manquants ou arrivant à échéance), regroupement et stockage d'éléments de preuve (p. ex. certifications, documents légaux, évaluations de la qualité, cotes de sécurité des installations ou des personnes, résultats des essais de produits, intégrité des états de service et documents de témoignages) concernant la capacité et l'expérience actuelles d'un fournisseur. Dans la plupart des cas, les justificatifs du fournisseur sont fournis par ce dernier dans une soumission.

Gestion des problèmes : processus qui comprend les activités requises pour diagnostiquer la cause racine des incidents et déterminer une résolution des problèmes. La gestion des problèmes est responsable de gérée le cycle de vie des problèmes par investigation, documentation et résolution.

Gestion des ressources : processus d'utilisation des ressources de la façon la plus efficiente possible. Paiement d'étape : Méthode de paiement progressif d'un élément mesurable ou défini (ou bien d'un ensemble de travaux ou d'un produit livrable).

Gestion des versions : méthodes et procédures pour l'intégration ainsi que pour le développement, la mise à l'essai, la mise en œuvre et le soutien de la solution.

H

Hôte : toute entité adressable du protocole Internet (IP) connectée à un réseau IP.

I

Incident : événement qui ne fait pas partie des activités normales d'un service et qui cause, ou pourrait causer, une interruption ou une réduction de la qualité d'un service.

Indicateur de rendement clé (IRC) : type de mesure de rendement servant à évaluer le succès d'une activité particulière.

Information protégée : désigne des dispositions particulières de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* et s'applique aux renseignements de nature délicate, privée et opérationnelle.

Infrastructure à clés publiques (ICP) : système complet requis pour fournir des services de chiffrement à clés publiques et de signature électronique pour une grande variété d'applications. Une organisation établit et maintient un environnement réseau fiable en gérant les clés et les certificats dans une ICP.

Infrastructure des SSI : ensemble du matériel, des logiciels et des installations qui servent au traitement et à la gestion de la solution.

Intégration : processus consistant à réunir les sous-systèmes de composantes dans un même système et à assurer que les sous-systèmes fonctionnent ensemble en tant que système unique.

Intégrité : exactitude et intégralité des renseignements et des biens et authenticité des transactions.

Intelligence d'affaires : ensemble de techniques et d'outils pour la transformation de données brutes en renseignements importants et utiles aux fins d'analyse des activités.

Interface de programme d'application (IPA) : ensemble de routines, de protocoles et d'outils servant à créer des applications, y compris des interfaces qui permettent aux composantes logiciel et matériel de communiquer entre elles.

Interface intuitive : Interfaces de la solution qui sont intuitives, comme il est défini ci-dessus (« intuitif ») pour les parties de la solution qui portent sur le service public Web vertical et frontal et l'application de traitement des services.

Interopérabilité : capacité de différents systèmes et de différentes applications à communiquer, à échanger des données et à utiliser les renseignements qui ont été échangés.

Intuitif : caractéristique souhaitable associée au concept de convivialité. Dans le cadre de la solution, l'adjectif « intuitif » signifie que l'utilisateur saisit rapidement ce qui se passe. Ceci signifie que l'utilisateur comprend rapidement le processus et les tâches précises exécutées sans que d'autres conseils, renseignements ou raisonnements déductifs soient nécessaires.

J-K

Jour ouvrable : tout jour de travail, du lundi au vendredi, à l'exclusion des jours fériés et d'autres congés, et de toute autre journée où le titulaire de licence est fermé.

L-M

Liste des certificats révoqués (LCR) : une infrastructure à clés publiques (ICP) qui précise les numéros de série uniques de tous les certificats révoqués. Avant d'utiliser un certificat, l'application utilisant des contrôles côté client doit vérifier la LCR appropriée pour déterminer si le certificat est toujours digne de confiance.

« Logiciel en tant que service » (SAAS) : capacité fournie au consommateur d'utiliser les applications du fournisseur qui sont sur une infrastructure en nuage. Les applications sont accessibles à partir de différents appareils du client par l'entremise d'une interface client légère comme un navigateur Web (p. ex. système de messagerie Web). Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, les unités de stockage ou même les capacités des applications, sauf, dans certains cas et de façon limitée, les paramètres de configuration d'applications propres à l'utilisateur.

Logiciel malveillant : tout logiciel utilisé pour interrompre le fonctionnement d'un ordinateur, obtenir des renseignements de nature délicate ou avoir accès à des systèmes informatiques privés. Hyperonyme utilisé pour désigner diverses formes de logiciels intrusifs comme les virus et les vers informatiques, les programmes troyens et les logiciels espions.

Marchandises contrôlées : définies à l'article de la *Loi sur la production de défense*. Cas d'utilisation : Outil d'analyse qui décrit les tâches qu'un système, une solution ou un service exécute pour un acteur ainsi que les buts que cet acteur atteindra à l'issue du processus (article 3).

Mesures : mesures de rendement qui évaluent les progrès et les tendances au sein d'une organisation.

Métadonnées : données qui définissent et décrivent d'autres données, et qui servent à identifier, à décrire, à localiser ou à utiliser les systèmes, les sources et les éléments d'information.

Modèle de données : organise les éléments de données (qualitatifs ou quantitatifs) et normalise la façon dont les éléments de données sont liés les uns aux autres. Un modèle de données détermine expressément la structure des données.

N

Niveau de classification : indicateur de la nature délicate des renseignements liés à la solution (p. ex. protégé A, protégé B, non classifié et autres classifications précisées par le gouvernement du Canada).

Notification : Message informant un utilisateur d'une action requise (p. ex. approuver, refuser, envoyer des documents à l'appui, etc.) ou qu'une action ayant été exécutée requiert de l'attention. Les notifications pourraient être produites par le système de la solution ou être des messages personnalisés par les utilisateurs internes.

Nouvelle version : version de système, nouvelle version et version provisoire d'un logiciel sous licence, que l'entrepreneur le désigne comme étant une « nouvelle version » ou non.

Numéro d'entreprise : numéro d'identification unique donné à une entreprise enregistrée par l'Agence du revenu du Canada.

O

P

Paramètre configurable : paramètre qui peut être modifié, prêt à l'emploi sans devoir être personnalisé, pour répondre aux normes et aux exigences du gouvernement du Canada, notamment en matière d'architecture des TI, des exigences fonctionnelles, de rendement, de disponibilité, de maintenabilité, de sécurité, de continuité des activités et de reprise après catastrophe.

Périmètre sécurisé : limite logique et physique autour des ressources et des renseignements du réseau qui sont accessibles, laquelle est contrôlée et protégée contre un accès non autorisé depuis l'extérieur de cette limite.

Personne autorisée : un citoyen canadien ou un résident permanent qui habite normalement au Canada qui fait des affaires au Canada ou qui est le représentant d'une entreprise qui cherche à obtenir/maintient en vigueur une inscription au Programme des marchandises contrôlées.

Plan d'essai d'acceptation : document qui décrit les scénarios de mise à l'essai, les activités et les résultats escomptés.

Plateforme : composantes générales de systèmes d'information utilisées pour traiter et stocker les données électroniques, comme les ordinateurs de bureau, les services, les appareils en réseau et les appareils mobiles. Les

plateformes sont en général constituées d'équipement serveur, de matériel de stockage, de matériel utilitaire, de logiciels et de systèmes d'exploitation.

Posture de sécurité : caractéristique d'un système d'information qui représente la capacité des contrôles de sécurité mis en œuvre de répondre aux besoins opérationnels en matière de sécurité et de contrer une menace.

Privilège d'utilisateur : autorisation accordée à un utilisateur de la solution qui lui permet d'accéder à des données/renseignements précis et de prendre des actions particulières Exemple de privilèges :

Privilège	Description
Créer	Créer un dossier
Lire	Visualiser un dossier
Inscrire	Apporter des modifications à un dossier
Supprimer	Supprimer un dossier
Ajouter	Lier un dossier à un autre dossier
Ajouter à	Associer un dossier à ce dossier
Attribuer	Transférer la responsabilité du dossier à un autre utilisateur
Échanger	Donner accès à un dossier à un autre utilisateur tout en conservant votre propre accès
Attribuer un autre parent	Attribuer un parent différent au dossier

Les utilisateurs qui ont délégué d'autres niveaux de contrôle sont appelés « utilisateurs privilégiés » (p. ex. administrateurs de système, ASSI). Les utilisateurs à qui il manque la plupart des privilèges sont définis comme étant des utilisateurs sans privilège, ordinaires ou normaux.

Profil d'utilisateur : document de données propres à l'utilisateur qui définit l'environnement et les rôles de travail de l'utilisateur.

Protégé A (information peu sensible) : s'applique à l'information qui, si elle est divulguée, pourraient raisonnablement causer un préjudice non lié à l'intérêt national, p. ex. divulgation du montant exact de salaires.

Protégé B (information particulièrement sensible) : s'applique aux renseignements qui, s'ils sont compromis, pourraient raisonnablement causer un préjudice grave relativement à un intérêt autre que national, p. ex. perte de réputation ou avantage concurrentiel.

Protégé C (information très sensible) : s'applique à la quantité très limitée d'information qui, si elle est compromise, pourrait raisonnablement cause un préjudice grave à un intérêt autre que national, p. ex. perte de vie.

Protocole de sécurité de la couche transport et son prédécesseur, protocole SSL, tout deux souvent appelés « SSL », sont des protocoles cryptographiques qui assurent la sécurité des communications dans un réseau informatique. Plusieurs versions des protocoles sont largement répandues dans les applications de navigation sur le Web, de courrier électronique, de télécopie par Internet, de messagerie instantanée et de voix sur IP (VoIP). Les grands sites Web utilisent le protocole de sécurité de la couche transport pour sécuriser toutes les communications entre les serveurs et les navigateurs Web.

Q-R

Rapports : génération de rapports standard, personnalisés ou ad hoc basés sur des domaines précis de renseignements requis qui sont affichés de la façon la plus appropriée possible.

Recherche booléenne dans les catalogues : vous permet de combiner des mots et des phrases au moyen des mots « AND », « OR » ou « NOT » (connus sous le nom d' « opérateurs booléens ») afin de limiter, d'élargir ou de raffiner votre recherche.

Recherche selon la logique floue : technique de retrait de texte basée sur la recherche de correspondances même quand les mots clés sont mal épelés ou donnent simplement une petite idée du concept.

Reçu : document original et copie électronique d'une copie certifiée indiquant le montant et la date d'une transaction comme preuve de paiement.

Registre principal : registre original à partir duquel des copies subséquentes sont effectuées.

Renseignement sensible : renseignement classifié ou désigné.

Renseignements classifiés : renseignements qui désignent des renseignements d'intérêt national susceptibles d'être visés par une exemption ou une exclusion en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, et dont la divulgation risquerait vraisemblablement de porter préjudice à l'intérêt national. Les catégories de classification comprennent « Confidentiel », « Secret » ou « Très secret » (voir les renseignements désignés).

Renseignements désignés : renseignements liés à des renseignements autres que d'intérêt national pouvant être admissibles à une exemption ou à une exclusion en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* Les catégories comprennent « protégé A » pour les renseignements de nature délicate, « protégé B » pour les renseignements de nature particulièrement délicate, ou « protégé C » pour les renseignements de nature extrêmement délicate (voir les renseignements classifiés).

Répartition des responsabilités : principe de sécurité selon lequel les responsabilités doivent être réparties lorsque c'est possible afin qu'aucune personne n'ait seul le contrôle sur une ressource ou un processus en particulier. Dans certains cas, il faut établir la coresponsabilité d'une ressource pour que sa manipulation ne soit possible que si une autre personne en a été informée.

Répertoire : endroit électronique où stocker et conserver des renseignements en toute sécurité aux fins de réutilisation dans la solution.

S

SABA : Une solution logicielle de gestion des talents qui comprend la gestion de l'apprentissage (SGA), la gestion du rendement et la collaboration en nuage.

Schéma de processus : explique et modélise les processus opérationnels qui sont exécutés par les utilisateurs, les rôles et les acteurs dans une entreprise.

Schéma : structure qui définit l'organisation des données dans une base de données.

Services en ligne de sécurité industrielle (SEDSI) Une application Web en ligne pour le dépôt de demandes d'attestation de sécurité du personnel.

Service public Web vertical et frontal : page Web spécialement conçue qui réunit les renseignements de diverses sources de manière uniforme. Habituellement, chaque source d'information occupe un endroit prévu à cet effet dans la page; souvent, l'utilisateur peut configurer quels renseignements afficher. Les variantes du service public Web vertical et frontal comprennent des « tableaux de bord » intranet pour les cadres et les gestionnaires.

Services Web : façon normalisée d'intégrer les applications Web au moyen des normes ouvertes XML, SOAP, WSDL et UDDI open standards dans le cadre d'un protocole Internet de base. Les services Web permettent aux organisations de communiquer des données sans devoir connaître de façon approfondie les systèmes de TI des autres organisations derrière le pare-feu.

Signature électronique : signature constituée d'une ou plusieurs lettres, d'un ou plusieurs caractères, chiffres ou autres symboles sous forme numérique qui sont incorporés dans un document électronique, joints à ce dernier ou qui y sont connexes.

Signature numérique : transformation cryptographique qui, lorsqu'elle est ajoutée à un message, une transaction ou un dossier, permet aux destinataires de vérifier la signature et de voir si les renseignements initiaux ont été modifiés ou si la signature a été contrefaite depuis que la transformation a eu lieu.

Spécifications de la conception : activités et produits livrables associés à la transformation des exigences systèmes liés aux utilisateurs et aux renseignements en spécifications techniques détaillées.

Système de production : complément de systèmes de TI en temps réel et de données réelles qui sont exécutés dans l'environnement de production utilisé au sein du gouvernement du Canada qui interagiront, communiqueront et exécuteront des programmes ou transféreront des données dans la solution afin traiter le travail quotidien du PSC et du PMC, et pour accommoder les activités associées à l'exécution d'un système ou plus de manière entièrement exposée, rendue disponible et appuyée pour les utilisateurs finaux et les utilisateurs visés desdits systèmes.

Système national de gestion de projet : Le Système national de gestion de projet (SNGP) est le cadre de gestion de projets de SPAC pour les *projets immobiliers* et *les projets axés sur la TI*. Le cadre du SNGP définit les principes clés et fournit les directives, les feuilles de route, les produits livrables et les outils nécessaires pour réaliser les projets dans le respect de la portée, des délais et du budget.

T

Tableau de bord : interface en temps quasi réel facile à lire, qui affiche l'état actuel (aperçu) de renseignements particuliers.

Tableau de bord : outil stratégique de gestion du rendement - un rapport structuré semi-standard, appuyé par des méthodes de conception et des outils d'automatisation qui peuvent être utilisés pour faire le suivi de l'exécution des activités et pour observer les conséquences qui découlent de ces actions.

Taxonomies : façon de classifier une structure et de l'attribuer à l'information.

Temps quasi réel : désigne le délai introduit, par le traitement de données automatisé ou la transmission réseau entre l'occurrence d'un événement et l'utilisation des données traitées, notamment pour l'affichage ou la rétroaction et à des fins de contrôle.

Territoires : région régie par un ensemble de lois en vertu d'un système de tribunaux ou d'entités gouvernementales qui diffèrent des régions voisines. Le Canada est une fédération de 11 territoires d'autorité gouvernementale distincts : le gouvernement fédéral et les 10 gouvernements provinciaux. Ils sont tous généralement indépendants les uns des autres en matière d'autorité législative.

Traçabilité : capacité de vérifier l'historique, l'emplacement ou l'application d'un élément au moyen de son identification enregistrée et documentée.

Transfert : passage de l'ancien système (matériel ou logiciel) au nouveau. Le transfert est le point auquel un nouveau système devient opérationnel.

U

UTF: (UTF-8) code de caractères permettant d'encoder tous les caractères possibles, ou points de code, définis dans Unicode. Le code est de longueur variable et utilise des unités de code de 8 bits.

Utilisateur autorisé : personne autorisée à effectuer des opérations dans le cadre de la solution.

Utilisateur externe : voir « utilisateur ». Les personnes qui n'utilisent pas le Secteur de la sécurité industrielle (SSI) qui accèdent aux services du SSI dans le cadre de la solution. Les rôles des utilisateurs externes sont notamment ceux d'agent de sécurité d'entreprise, d'agent de sécurité du gouvernement du Canada, d'agent de sécurité étranger, de représentants désignés, etc.

Utilisateur interne : voir « utilisateur ». Employés du SSI qui utilisent la solution pour fournir des services du PSC/PMC aux utilisateurs externes. Les utilisateurs internes sont notamment les agents d'enregistrement, les agents d'enquête de sécurité, les inspecteurs, les enquêteurs, etc.

Utilisateur privilégié : utilisateur qui en raison de sa fonction peut obtenir des privilèges d'accès améliorés à la solution afin qu'il puisse la mettre à jour ou exécuter des tâches administratives. (p. ex. administrateurs de systèmes, administrateurs de bases de données, agents de sécurité des systèmes d'information, etc.)

Utilisateur : toute personne qui est enregistrée auprès d'un compte pour utiliser la solution.

Type d'utilisateur	Exemples
Utilisateur externe	**Clients SSI :** agents de sécurité d'entreprise, représentants désignés, personnes autorisées, etc. Partenaires SSI : agents de sécurité des groupes Services (GS), agents d'approvisionnement du gouvernement du Canada, agents de sécurité étrangers, etc.
Utilisateur externe	**Agents du programme PSC/PMC** : agents d'enregistrement, agents, de vérification du personnel de sécurité, inspecteurs, enquêteurs, etc.
Utilisateur privilégié	Administrateurs de système, agents de sécurité des systèmes d'information, etc.

V

Visualisation des données : méthode servant à mettre les données dans un contexte visuel ou pictural comme moyen de communiquer les renseignements aux utilisateurs de façon claire et efficace (p. ex. une carte est une façon de visualiser quelles parties du pays reçoivent le plus de pluie).

W

X-Y-Z

Fichier ZIP : dossier électronique de fichiers comprimés.

APPENDICE 6 DE L'ANNEXE A – ACRONYMES ET ABRÉVIATIONS

APPENDICE 6 DE L'ANNEXE A – ACRONYMES ET ABRÉVIATIONS

Le présent appendice contient les acronymes et les abréviations utilisés dans l'*ANNEXE A – Énoncé des travaux (EDT)*. Il doit être utilisé en conjonction avec l'*appendice 5 de l'ANNEXE A : Glossaire des termes.*

AA	Accès amélioré
AA-GC	Agent des achats du gouvernement du Canada
AC	Accès complet
ADR	Autorisation de détenir des renseignements
ADS	Administration désignée en matière de sécurité
AM	Autres ministères
AMC	Affaires mondiales Canada
ANS	Administration nationale de la sécurité
AOS	Architecture orientée services
ARSE	Agent de sécurité d'entreprise suppléant
ARSI	Agent régional de la sécurité industrielle
ARSI	Agent régional de la sécurité industrielle
ASA	Accès au secteur d'activité
ASE	Agent de sécurité d'entreprise
ASE	Agent de sécurité étranger
ASFC	Agence des services frontaliers du Canada
AS-GC	Agent de sécurité du gouvernement du Canada
ASI	Attestation de sécurité de l'installation
ASU	Agent de sécurité de l'unité
ASV	Attestation de sécurité de visite
BARG	Bouton d'achat du Receveur général
BGP	Bureau de gestion de projet
BMA	Bureau mixte d'agrément des États-Unis et du Canada

BPR	Bureau de première responsabilité
BSO	Bureau de sécurité de l'OTAN
CAC	Cote d'accès au chantier
CCSIG	Comité consultatif sur la sécurité industrielle du gouvernement
CDSS	Conception détaillée des services de sécurité;
CF	Cote de fiabilité
CGSS	Conception générale des services de sécurité
COSMIC	NATO Très secret
COTS	Produit commercial
CPI	Centre de protection de l'information
CSP	Cadre supérieur clé
CST	Centre de la sécurité des télécommunications
CVDL	Cycle de vie de développement des systèmes
DAE	Direction des analyses et des enquêtes
DE	Déroulement des activités
DFSP	Division du filtrage de la sécurité du personnel
DGDPI	Direction générale du dirigeant principal de l'information
DGS	Direction générale de la surveillance
DIE	Direction des inspections et des enquêtes
DMC	Direction des marchandises contrôlées
DP	Demande de propositions
DPI	Dirigeant principal de l'information
DSIC	Direction de la sécurité industrielle canadienne
DSII	Direction de la sécurité industrielle internationale
DV	Demande de visite

EAS	Évaluation et autorisation de sécurité
EAU	Essai d'acceptation par l'utilisateur
EDI	Échange de données informatisées
EDT	Énoncé des travaux
EMR	Évaluation des menaces et des risques
END	Entente de non-divulgation
ESB	Bus de service d'entreprise
ESOSP	Enquête de sécurité sur une organisation du secteur privé
ESP	Enquêtes de sécurité sur le personnel
ETC	Extraire, transformer et charger
FAQ	Foire aux questions
FIS	Feuillet d'information – Attestation de sécurité de personne
FP	Service professionnel
GC	Gouvernement du Canada
GCPE	Gestion de cas et pratiques exemplaires
GI/TI	Gestion de l'information et technologie de l'information
GJE	Gestion des justificatifs externes
GJI	Gestion des justificatifs internes
GPA	Gestion de programmes et Apprentissage
GPO	Gestion des processus opérationnels
GRC	Gestion des relations avec les clients
GRC	Gendarmerie royale du Canada
GSTI	Gestion de la sécurité des technologies de l'information
HP	Hors du pays
ICP	Infrastructure à clés publiques

IGU	Interface graphique utilisateur
IPA	Interface de programmation des applications
IRC	Indicateur de rendement clé
IS	Intégrateur de systèmes
ITAR	*International Traffic in Arms Regulations*
ITSG	Lignes directrices en matière de sécurité des technologies de l'information
LCR	Liste des certificats révoqués
LDAP	Lightweight Directory Access Protocol
LMEC	Liste des marchandises d'exportation contrôlée
LO	Langues officielles
LPD	*Loi sur la production de défense*
LPRPDÉ	*Loi sur la protection des renseignements personnels et les documents électroniques*
LS	Logiciel comme service
LS	Logiciel comme service
LVERS	Liste de vérification des exigences relatives à la sécurité
LVERS en ligne	Liste de vérification des exigences relatives à la sécurité en ligne
MDN	Ministère de la Défense nationale
MS	Microsoft
MSI	Manuel de la sécurité industrielle
NCD	Numéro de contrôle du document (empreintes)
NNN	Ressortissant d'un pays non membre de l'OTAN
OSSI	Officier de sécurité du système d'information
OTAN	Organisation du Traité de l'Atlantique Nord
PA	Personne autorisée

PA	Personnel affecté
PAOS	Protocole SOAP (Simple Object Access Protocol)
PCRD	Programme de certification des représentants désignés
PDF	Format de document portable
PE	Protocole d'entente
PESI	Protocole d'entente sur la Sécurité industrielle
PIGC	Plateforme d'interopérabilité du gouvernement du Canada
PMA	Programme mixte d'agrément des États-Unis et du Canada
PMC	Programme des marchandises contrôlées
PRO	Planification des ressources de l'organisation
PSC	Programme de sécurité des contrats
PSG	Politique sur la sécurité du gouvernement
PSI	Programme de la sécurité industrielle
PU	Présentation uniforme
RA	Renseignements d'affaires
RCN	Région de la capitale nationale
RD	Représentant désigné
RH	Ressources humaines
RMC	*Règlement sur les marchandises contrôlées*
ROD	Dissipation des doutes
ROEM	Renseignement d'origine électromagnétique
ROW	Limité à son propre travail
SACI	Service d'authentification centralisé interne
SAE	Solution d'approvisionnement électronique

SCIASP	Système de collecte d'information pour les attestations de sécurité de personnel
SCRS	Service canadien du renseignement de sécurité
SCT	Secrétariat du Conseil du Trésor
SE	Système d'exploitation
SÉCOM	Sécurité des communications électroniques
SEDSI	Services en direct de sécurité industrielle
SFSP	Service en direct de filtrage de sécurité du personnel
SGCP	Système de gestion de cas partagé
SGIJA	Solution de gestion de l'identité, des justificatifs et de l'accès
SGTSF	Services gérés de transfert sécurisé de fichiers
SIEM	Gestion des événements et des informations de sécurité
SMS	Service de messages courts
SNGP	Système national de gestion de projet
SPAC	Services publics et Approvisionnement Canada
SPC	Services partagés Canada
SRT	Structure de répartition du travail
SRTM	Matrice de traçabilité des exigences en matière de sécurité du système
SSI	Secteur de la sécurité industrielle
TDL	Trousse de développement logiciel
TI	Technologie de l'information
TLS	Protocole TLS (Transport Layer Security)
TPSGC	Travaux publics et Services gouvernementaux Canada
TSSI	Transformation des systèmes de sécurité industrielle
URES	Unité responsable des enquêtes de sécurité

VDEL	Vérification des dossiers sur l'exécution de la loi
VOD	Vérification d'organisation désignée

ANNEXE B – BARÈME DE PRIX

1. Directives [Ces directives seront retirées à l'attribution du contrat, et le barème de prix sera renuméroté en conséquence.] **:**

1.1 Les soumissionnaire est prié de soumettre, avec son financière du soumissionnaire, le formulaire 3 de la partie 4, Demande de soumissions - Formulaire de soumission financière, dûment rempli.
1.2 Les soumissionnaires ne devraient pas utiliser les tableaux ci-dessous dans leur soumission financière.
1.3 Le barème de prix du contrat sera élaboré en fonction des données saisies dans le formulaire 3 de la partie 4, Demande de soumissions – Formulaire de barème de prix du soumissionnaire retenu.

2. Présentation

L'entrepreneur sera payé pour les travaux effectués selon la base de paiement du contrat, conformément aux travaux à prix ferme indiqués dans les parties 1, 2, 3, 4, 5, 6, 7, et 8 de l'ANNEXE A - Énoncé des travaux et chaque autorisation de tâches approuvée. Les estimations accompagnant chaque autorisation de tâches doivent respecter l'article 7.2, Autorisation de tâches, qui sera ensuite calculé conformément aux taux indiqués dans la présente ANNEXE B.

3. Prix de lot ferme – Les sections 1 à 8 de l'ANNEXE A, Énoncé des travaux

Le fournisseur sera payé selon un prix de lot ferme pour les travaux effectués aux termes du contrat et du tableau 1 ci-dessous.

Les prix sont en dollars canadiens, droits de douane inclus et taxes applicables en sus.

Tableau 1 – Prix de lot ferme et Calendrier de paiements d'étape Sections 1 à 8 de l'ANNEXE A, Énoncé des travaux (aux fins de l'évaluation financière)			
(A) Description de l'étape	**(B) Montant (en $ CA)**	**(C) Livrables de l'étape**	**(D) Date d'échéance**
1	$0.00		
2	$0.00		
3	$0.00		
…	$0.00		
n	$0.00		
(E) Prix de lot ferme total [somme de la colonne (B) pour toutes les étapes, de 1 à n]	**$0.00**		

4. Travaux sur demande

L'entrepreneur sera payé conformément aux tarifs journaliers fermes du tableau 2 pour les travaux effectués dans le cadre du contrat et de toute autorisation de tâches subséquente.

Les prix sont en dollars canadiens, droits de douane inclus et taxes applicables en sus.

Tableau 2 - Travaux sur demande (article 9 de l'ANNEXE A, Énoncé des travaux) – Autorisation de Tâches – Catégories de ressources		
Catégories de ressources	**De l'attribution de la période initiale du contrat au (la date de fin sera insérée à l'attribution du contrat) – Tarif journalier ferme tout compris ($ CA)**	**Périodes d'options 1, 2, 3, 4 (les dates de début et de fin seront insérées à l'attribution du contrat) – Tarif journalier ferme tout compris ($ CA)**
1. Expert-conseil en communications (Niveau 3)		
2. Développeur de didacticiel (Niveau 3)		
3. Spécialiste en conversion de données (Niveau 3)		
4. Administrateur de bases de données (Niveau 3)		
5. Modélisateur de données (Niveau 3)		
6. Architecte en Gestion Information (Niveau 3)		
7. Programmeur / Analyste (Niveau 3) – SAP Business Objects		
8. Programmeur / Analyste (Niveau3) – MS Dynamics CRM		
9. Développeur de page Web (Niveau 3)		
10. Expert-conseil en restructuration des processus opérationnels (Niveau 3)		
11. Expert-conseil en gestion du changement (Niveau 3)		
12. Spécialiste de la cybersécurité (Niveau 3)		
13. Spécialiste de la gestion des incidents (Niveau 3)		
14. Spécialiste de la conception de la sécurité des TI (Niveau 3)		
15. Ingénieur en sécurité des TI (Niveau 3)		
16. Spécialiste des analyses de vulnérabilité de la sécurité des TI (Niveau 3)		
17. Analyste de réseau (Niveau 3)		
18. Spécialiste du soutien des opérations (Niveau 3)		
19. Vérificateur de systèmes (Niveau 3)		
20. Coordonnateur des essais (Niveau 3)		
21. Concepteur Web (Niveau 3)		
22. Programmeur ou développeur de logiciels (Niveau 3)		

Tableau 2 - Travaux sur demande (article 9 de l'ANNEXE A, Énoncé des travaux) – Autorisation de Tâches – Catégories de ressources		
Catégories de ressources	**De l'attribution de la période initiale du contrat au (la date de fin sera insérée à l'attribution du contrat) – Tarif journalier ferme tout compris ($ CA)**	**Périodes d'options 1, 2, 3, 4 (les dates de début et de fin seront insérées à l'attribution du contrat) – Tarif journalier ferme tout compris ($ CA)**
23. Architecte d'applications et de logiciels (Niveau 3)		
24. Analyste de bases de données (Niveau 3)		

ANNEXE F – RENSEIGNEMENTS SUR LES CATÉGORIES DE RESSOURCES DANS LE CADRE DES SERVICES FACULTATIFS

1. Considérations générales

La présente annexe vise à décrire l'expertise et les compétences minimales obligatoires des diverses catégories de ressources qui peuvent être réquises «sur demande», conformément au contrat, aux AT, à l'*ANNEXE A, Énoncé des travaux* et à l'ANNEXE *B, Barème de prix*.

On parle ici des catégories suivantes :

1. Expert-conseil en communications (Niveau 3);
2. Développeur de didacticiel (Niveau 3);
3. Spécialiste en conversion de données (Niveau 3);
4. Administrateur de bases de données (Niveau 3);
5. Modélisateur de données (Niveau 3);
6. Architecte en Gestion Information (Niveau 3);
7. Programmeur / Analyste (Niveau 3) – SAP Business Objects;
8. Programmeur / Analyste (Niveau3) – MS Dynamics CRM;
9. Développeur de page Web (Niveau 3);
10. Expert-conseil en restructuration des processus opérationnels (Niveau 3);
11. Expert-conseil en gestion du changement (Niveau 3);
12. Spécialiste de la cybersécurité (Niveau 3);
13. Spécialiste de la gestion des incidents (Niveau 3);
14. Spécialiste de la conception de la sécurité des TI (Niveau 3);
15. Ingénieur en sécurité des TI (Niveau 3);
16. Spécialiste des analyses de vulnérabilité de la sécurité des TI (Niveau 3);
17. Analyste de réseau (Niveau 3);
18. Spécialiste du soutien des opérations (Niveau 3);
19. Vérificateur de systèmes (Niveau 3);
20. Coordonnateur des essais (Niveau 3);
21. Concepteur Web (Niveau 3);
22. Programmeur ou développeur de logiciels (Niveau 3);
23. Architecte d'applications et de logiciels (Niveau 3); et
24. Analyste de bases de données (Niveau 3).

Les catégories de ressources supplémentaires peuvent être identifiées et demandées pendant la durée du contrat. Les services requis et les compétences minimales obligatoires pour les autres catégories de ressources des Services professionnels seront élaborées. Les catégories de ressources supplémentaires sont assujetties aux compétences minimales obligatoires.

2. Curriculum vitæ des ressources proposées en réponse aux autorisations de tâches :

Sauf indication contraire dans le contrat, la réponse de l'entrepreneur à une AT ou à une AT révisée doit comprendre les curriculum vitæ des ressources proposées. Dans ceux-ci, on doit faire la preuve que chaque personne proposée satisfait aux exigences décrites (études, expérience de travail et accréditation professionnelle). Voici les éléments à considérer quant aux curriculum vitæ et aux ressources :

(a) Parmi les ressources proposées, on peut compter des employés de l'entrepreneur ou d'un sous-traitant ainsi que des entrepreneurs indépendants auxquels l'entrepreneur confierait une partie des travaux.

(b) Dans le cas des exigences en matière de formation (diplôme, certificat, agrément), seuls les programmes de formation terminés par la ressource au moment de la soumission en réponse à l'AT seront pris en considération.

(c) En ce qui concerne les exigences relatives aux titres professionnels, la ressource doit détenir le titre exigé au moment de la soumission en réponse à l'AT et doit demeurer, le cas échéant, un membre en règle de l'organisme professionnel en question pendant la durée de l'AT.

(d) L'entrepreneur doit décrire précisément à quel endroit, à quel moment (mois et année) et de quelle façon (activités, responsabilités) la personne en question a acquis les compétences ou l'expérience exigées dans les présentes.

(e) Le Canada peut exiger une preuve de la réussite de la formation officielle ainsi que des renseignements de référence. Le Canada peut effectuer un contrôle des références pour vérifier l'exactitude des renseignements fournis. Le cas échéant, ce contrôle sera fait par courriel (sauf si la personne citée en référence n'est accessible que par téléphone). Le Canada ne jugera pas qu'une exigence obligatoire est respectée à moins que la réponse soit reçue dans les cinq jours ouvrables. Le troisième jour ouvrable après l'envoi du courriel, si le Canada n'a pas reçu de réponse, il en informera le soumissionnaire par courriel pour que ce dernier puisse rappeler à la personne en question qu'il faut répondre au Canada dans le délai de cinq jours ouvrables prescrit. Si les renseignements fournis par une personne citée en référence diffèrent des renseignements fournis par l'entrepreneur, les renseignements fournis par la personne citée en référence seront les renseignements évalués. Une exigence obligatoire ne sera pas considérée comme étant respectée si le client cité en référence n'est pas un client de l'entrepreneur (par exemple, le client ne peut être un client d'une société affilée de l'entrepreneur). De même, on considérera qu'une exigence obligatoire n'est pas respectée si le client est lui-même une filiale ou une autre entité ayant un lien de dépendance avec l'entrepreneur. Des références de l'État seront acceptées.

(f) Pendant l'évaluation des ressources proposées, si les références de deux ressources ou plus nécessaires dans le cadre de l'AT ne fournissent pas de réponse ou ne justifient pas les compétences exigées pour la prestation des services requis, l'autorité contractante peut déclarer l'offre de prix irrecevable.

3. Exigences et services requis dans le cadre des autorisations de tâches

3.1 Expert-conseil en communications (Niveau 3)

3.1.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) planifier, étudier, modifier, rédiger ou examiner des notes, des textes, des simulations, des reportages, des discours, des guides, des devis et d'autres articles à caractère non journalistique, ou y participer, en conformité avec les normes établies;
(b) élaborer et mettre en œuvre des plans stratégiques de communication au sein d'organismes dispersés géographiquement en transformation organisationnelle (gestion du changement);
(c) fournir des conseils quant à la consultation en communications afin d'appuyer les initiatives et les stratégies de communication stratégique;
(d) créer le matériel de soutien des communications;
(e) développer et mettre en œuvre des produits créatifs de communication et d'information à l'aide d'une variété d'outils, de techniques et de supports, et sélectionner un moyen approprié pour faire passer l'information, les idées et les résultats;
(f) élaborer et mettre en œuvre les stratégies et les plans de communications;
(g) émettre et échanger de l'information de manière claire et concise;
(h) veiller à ce que l'information soit communiquée aux personnes compétentes en temps opportun;
(i) rédiger les rapports à des fins précises dans un langage clair, communicatif et professionnel (p. ex., rapports de vérification, lettres de gestion, rapports de consultation, rapports financiers);
(j) veiller à ce que les communications soient bien comprises en encourageant et en écoutant les commentaires provenant de l'intérieur et de l'extérieur de l'organisation;
(k) structurer les communications externes de façon à véhiculer une image ministérielle appropriée;
(l) assurer la confidentialité de l'information et des données organisationnelles et des clients;

(m) déterminer les publics cibles afin de mieux concevoir les messages;
(n) établir et déterminer les obstacles et les barrières aux communications;
(o) donner des conseils sur des questions touchant les approches ou les options liées à l'élaboration de programmes et de politiques et les options de planification des communications (interne ou externe);
(p) rechercher, développer et mettre en œuvre des stratégies de communication impliquant les médias sociaux et leur contenu associé (c.-blogs, microblogs, les wikis, externalisation ouverte, les communautés de contenu, réseaux sociaux, etc);
(q) fournir un soutien et aider les communicateurs à utiliser les médias sociaux pour compléter les canaux traditionnels;
(r) fournir des suggestions sur la réduction des coûts dans le processus de communication.

3.1.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Expert-conseil en communications.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (c), (d), (e),(f),(h), (m), (n) et (o) de 3.1.1.

3.2 Développeur de didacticiel (Niveau 3)

3.2.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Surveiller toutes les installations du processus de conversion. Effectuer des évaluations ou des analyses des besoins en matière de formation.
(b) Planifier et surveiller les projets de formation.
(c) Effectuer l'analyse du contenu, du travail et de la tâche.
(d) Élaborer des objectifs à partir des critères d'écriture et du rendement.
(e) Recommander le médium d'enseignement et des stratégies d'enseignement.
(f) Élaborer des instruments de mesure de rendement.
(g) Élaborer du matériel pour le programme de formation.
(h) Préparer les utilisateurs à la mise en œuvre du didacticiel.
(i) Communiquer efficacement sous forme visuelle, orale et écrite avec des individus, des petits groupes et de grands auditoires.

3.2.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Développeur de didacticiel.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (c), (e), (g) et (h) de 3.2.1.

3.3 Spécialiste en conversion de données (Niveau 3)

3.3.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Surveiller toutes les installations du processus de conversion.
(b) Effectuer le mappage, les interfaces, le travail de conversion simulée, les améliorations, le processus de conversion en soi, et vérifier la complétude et l'exactitude des données transformées.
(c) Créer de bons liens de travail avec tous les clients, communiquer efficacement avec tous les niveaux de personnel/clients, et fournir un soutien de conversion.
(d) Analyser et coordonner la conversion des fichiers de données.
(e) Importer les fichiers des plateformes hétérogènes.

3.3.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Spécialiste en conversion de données.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (d) et (e) de 3.3.1.

3.4 Administrateur de bases de données (Niveau 3)

3.4.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Adapter les routines de conversion des bases de données.
(b) Peaufiner la stratégie de conversion.
(c) Générer une nouvelle base de données avec le client.
(d) Mettre à jour les dictionnaires de données.
(e) Élaborer et mettre en œuvre les procédures qui assureront l'exactitude et la complétude des données emmagasinées dans la base de données, ainsi que la possibilité d'y accéder dans un délai raisonnable.
(f) Élaborer et mettre en œuvre des procédures de sécurité relatives à la base de données, incluant l'accès et la gestion des comptes des utilisateurs.
(g) Maintenir à jour le contrôle de la configuration de la base de données.
(h) Effectuer ou coordonner les mises à jour de la conception de la base de données.
(i) Contrôler et coordonner les modifications à la base de données, y compris la suppression d'enregistrements, la modification d'enregistrements existants et les ajouts à la base de données.
(j) Élaborer et coordonner les procédures de copie de renfort, de reprise des activités et de protection antivirus.

3.4.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Administrateur de bases de données.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (e), (f), (h) et (j) de 3.4.1.

3.5 Modélisateur de données (Niveau 3)

Le modélisateur de données a la responsabilité stratégique et tactique de l'élaboration et le maintien des modèles architecturaux et de données pour les initiatives du ministère et des projets spécifiques. Ceci inclut l'identification des données les plus utiles au ministère, l'intégration de ces données, et l'élaboration des modèles de données fondamentales de liaison. Les modèles de données qui en résultent se baseront sur les principes de l'architecture de données et de la conception de modélisation.

3.5.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Définir, élaborer et tenir à jour des modèles logiques de données.
(b) Analyser des modifications proposées aux bases de données dans le contexte du modèle logique de données.
(c) Fournir des conseils techniques en ce qui concerne l'utilisation optimale des techniques de modélisation des données aux membres de l'équipe.
(d) Offrir de l'aide technique, de l'encadrement et de l'orientation relatifs à l'analyse et la modélisation des données aux membres de l'équipe.
(e) Offrir de l'aide aux utilisateurs dans les équipes de projet et aux utilisateurs fonctionnels relativement aux problèmes de données et des notions d'analyse de données.
(f) Participer à l'élaboration de politiques et de procédures en matière de la modélisation des données et des metadonnées.
(g) Participer à l'analyse des données suite à des modifications d'exigences ou des mises à jour.
(h) Mettre en œuvre les modifications approuvées aux modèles logiques de données.
(i) Tenir compte des architectures, des stratégies et des cadres de données de l'entreprise, y compris le stockage des données de l'entreprise.
(j) Analyser et évaluer des solutions alternatives en architecture des données pour satisfaire aux exigences/problèmes de l'entreprise à intégrer dans l'architecture des données de l'entreprise.
(k) Réviser les stratégies et les orientations d'architecture de l'entreprise, les exigences relatives aux données, et les besoins en information de l'entreprise et concevoir des structures pour les appuyer.
(l) Améliorer l'efficacité de la modélisation par l'entremise de recommandations sur une meilleure utilisation des dépôts de metadonnées en place.
(m) Se conformer aux directives sur les dépôts de metadonnées de l'entreprise.
(n) Formuler des commentaires sur l'amélioration des architectures des données.
(o) Contribuer à l'amélioration des architectures des données.
(p) Définir des stratégies d'accès.
(q) Établir, contrôler et faire un rapport sur les plans et les calendriers de travail.

3.5.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Modélisateur de données.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (c), (d), (e), (g), (i) et (j) de 3.5.1.

3.6 Architecte en Gestion Information (GI) (Niveau 3)

3.6.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Analyser les capacités et les besoins existants, élaborer des cadres conçus à nouveau et recommande des secteurs où améliorer la capacité et l'intégration.
(b) Élaborer et réviser des énoncés détaillés des besoins.
(c) Évaluer les procédures et les méthodes existantes, identifier et documenter le contenu de la base de données, la structure et les sous-systèmes d'applications, et élaborer des dictionnaires de données.

(d) Définir et documenter les interfaces entre les opérations manuelles et automatisées dans les sous-systèmes d'applications, avec les systèmes de l'extérieur et entre les nouveaux systèmes et les systèmes en place.
(e) Faire le prototype de solutions possibles, informer sur les compromis et recommander des options.
(f) Effectuer de la modélisation d'informations en vue d'appuyer la mise en œuvre du RMA.
(g) Effectuer des analyses de rentabilité en ce qui concerne la mise en œuvre de nouveaux procédés et de nouvelles solutions.
(h) Offrir des conseils sur l'élaboration et l'intégration des modèles de procédés et d'information avec les procédés visant à éliminer les redondances d'information et de procédés.
(i) Offrir des conseils sur la définition de nouvelles exigences et de nouvelles possibilités de mettre en pratique des solutions efficaces ; déterminer les options possibles et fournir les coûts préliminaires.

3.6.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Architecte en GI.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (d) et (h) de 3.6.1.

3.7 Programmeur/Analyste (Niveau 3) – SAP Business Objects

3.7.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Élaborer et modifier le code et le logiciel.
(b) Élaborer et modifier les écrans et les rapports.
(c) Faire la cueillette des données et les analyser dans le cadre d'étude visant à établir la faisabilité technique et la faisabilité financières de systèmes informatiques proposés et dans le cadre de l'élaboration de spécifications fonctionnelles et de conception de système.
(d) Concevoir des méthodes et des procédures relatives à des systèmes informatiques de petite envergure et à des sous-systèmes de systèmes de plus grande envergure.
(e) Élaborer des systèmes informatiques de petite envergure et des sous-systèmes de plus grande envergure, en faire l'essai et les mettre en œuvre.
(f) Produire des formulaires, des manuels, des programmes, des fichiers de données et des procédures pour des systèmes et/ou des applications.

3.7.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Programmeur/Analyste.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (c), (d), et (e) de 3.7.1.
O4	Doit avoir au moins trois (3) années d'expérience, au cours des dix (10) dernières années, à développer des rapports de business intelligence à l'aide de Business Objects de SAP.

3.8 Programmeur/Analyste (Niveau 3) – MS Dynamics CRM

3.8.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Élaborer et modifier le code et le logiciel.
(b) Élaborer et modifier les écrans et les rapports.
(c) Faire la cueillette des données et les analyser dans le cadre d'étude visant à établir la faisabilité technique et la faisabilité financières de systèmes informatiques proposés et dans le cadre de l'élaboration de spécifications fonctionnelles et de conception de système.
(d) Concevoir des méthodes et des procédures relatives à des systèmes informatiques de petite envergure et à des sous-systèmes de systèmes de plus grande envergure.
(e) Élaborer des systèmes informatiques de petite envergure et des sous-systèmes de plus grande envergure, en faire l'essai et les mettre en œuvre.
(f) Produire des formulaires, des manuels, des programmes, des fichiers de données et des procédures pour des systèmes et/ou des applications.

3.8.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Programmeur / Analyste.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (c), (d), et (e) de 3.8.1.
O4	Doit avoir au moins trois (3) années d'expérience, au cours des dix (10) dernières années, à concevoir, développer et mettre en œuvre des systèmes utilisant MS Dynamics CRM.

3.9 Développeur de page Web (Niveau 3)

3.9.1 Services requis

Les services requis peuvent comprendre notamment, sans toutefois s'y limiter, ce qui suit :

(a) Develop and Élaborer et préparer des plans sous forme de diagrammes en ce qui concerne la prestation de services sur Internet.
(b) Analyser les problèmes décrits par les analystes et les concepteurs de systèmes concernant des facteurs comme le style et la quantité d'information à transmettre sur Internet.
(c) Choisir et utiliser les meilleurs outils d'élaboration de page Web offerts pour lier le client sur Internet aux programmes de prestation d'information et aux bases de données « dorsaux » du ministère.
(d) Concevoir des pages Web à employabilité élevée en vue de combler les besoins.
(e) Vérifier l'exactitude et la complétude des programmes en préparant des échantillons de données et en les essayant à l'aide d'essais effectués par le personnel de service.
(f) Corriger les erreurs de programmation en révisant les instructions ou en changeant la séquence des opérations.
(g) Produire les instructions et assembler les spécifications, les ordinogrammes, les diagrammes, les présentations, la programmation et les instructions de fonctionnement en vue de documenter les applications pour modification ou consultation ultérieures.

3.9.2 Compétences minimales obligatoires

No.	Description des critères
O1	Doit avoir au moins dix (10) ans d'expérience en tant que Développeur de page Web.
O2	Doit posséder un diplôme universitaire ou un diplôme collégial (dans n'importe quel domaine).
O3	Doit avoir au moins cinq (5) années d'expérience, au cours des dix (10) dernières années, exécutants les responsabilités décrites dans les sections (a), (b), (c), et (d) de 3.9.1.
O4	Doit avoir au moins trois (3) années d'expérience, au cours des dix (10) dernières années, en développement des services basée sur le Web en utilisant Adxstudio Portals.

3.10 Expert-conseil en restructuration des processus opérationnels (Niveau 3)

3.10.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Examiner la structure organisationnelle et les processus de travail existants.
b) Analyser les exigences fonctionnelles opérationnelles en vue de déterminer l'information, les procédures et les processus décisionnels.
c) Cerner les processus susceptibles d'être conçus à nouveau, créer le prototype des solutions possibles, fournir de l'information sur les compromis et recommander une option à suivre. Déterminer les modifications à apporter aux processus automatisés.
d) Offrir des conseils spécialisés sur la définition de nouvelles exigences et de nouvelles possibilités de mettre en pratique des solutions efficaces. Déterminer les options possibles et fournir les coûts préliminaires.
e) Offrir des conseils spécialisés sur l'élaboration et l'intégration des modèles de processus et d'information afin d'éliminer les redondances dans les processus et l'information.
f) Déterminer et recommander de nouveaux processus et de nouvelles structures organisationnelles.
g) Fournir des conseils spécialisés et un appui concernant la mise en place de nouveaux processus et de changements organisationnels.
h) Consigner les flux des travaux.
i) Utiliser des outils logiciels de modélisation des opérations, des flux des travaux et de l'organisation.

3.10.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins dix (10) ans d'expérience en tant qu'expert-conseil en restructuration des processus opérationnels.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b), c), e) et g) de la section 3.10.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.11 Expert-conseil en gestion du changement (Niveau 3)

3.11.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Concevoir des interventions visant à améliorer l'efficacité organisationnelle au moyen de changements axés sur le système.
b) Concevoir des interventions qui contribuent à améliorer l'efficacité organisationnelle au moyen de changements axés sur les personnes et garants de transformation, d'un meilleur environnement, d'une participation accrue et d'un effectif plus souple.
c) Élaborer et mettre en œuvre des stratégies, des plans et un cadre de gestion du changement.
d) Choisir des outils de gestion de changement et déterminer les risques.
e) Offrir de l'expertise, des conseils consultatifs, de l'orientation et de l'encadrement dans le but de constituer la capacité du projet afin d'utiliser efficacement les stratégies de gestion du changement et les outils connexes.

f) Présenter l'objectif des changements de manière que le personnel en comprenne le sens et qu'il projette une image attrayante de la nouvelle organisation.
g) Concevoir et réaliser une évaluation de l'état de préparation au changement en vue de planifier et de mettre en œuvre une stratégie de gestion du changement.
h) Encadrer les membres du personnel en leur faisant sentir que leur contribution compte au sein de la nouvelle organisation.
i) Évaluer l'efficacité de l'initiative de gestion du changement.
j) Élaborer les cadres d'évaluation et de mesure de rendement.
k) Intégrer des disciplines de surveillance de rendement dans un plan de gestion du changement et de développement d'organisation.
l) Surveiller le rendement en matière de gestion du changement et en rendre compte.

3.11.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins dix (10) ans d'expérience en tant qu'expert-conseil en gestion du changement.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b), c), d), g), i), j) et k) de la section 3.11.1.

3.12 Spécialiste de la cybersécurité (Niveau 3)

3.12.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Élaborer une conception de solution de sécurité (niveau élevé et niveau de détail).
b) Élaborer des plans de sécurité comme un plan d'installation de sécurité, un plan d'essai de sécurité, un plan de vérification d'installation de sécurité et un plan d'évaluation de vulnérabilité.
c) Effectuer des activités d'évaluation de la menace et des risques (EMR) au cours du cycle de développement de la solution.
d) Élaborer des procédures, telles que des procédures de sécurité opérationnelle et des procédures d'installation de sécurité.
e) Élaborer et tenir à jour la grille de traçabilité des exigences de sécurité.
f) Préparer des rapports de sécurité, tels que des rapports d'EMR, des rapports de vérification de l'installation de sécurité et des rapports d'essai d'intégration de sécurité.
g) Préparer des trousses de sécurité des TI pour les points de contrôle de l'Évaluation et autorisation de sécurité (EAS).
h) Former des développeurs sur des pratiques de codage de sécurité afin d'intégrer la connaissance de la sécurité dans un processus de développement.

3.12.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins (10) ans d'expérience en tant que spécialiste de la sécurité des TI.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b), c) et d) de la section 3.12.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.13 Spécialiste de la gestion des incidents (Niveau 3)

3.13.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Examiner, analyser et appliquer :
   - les analyseurs de réseau et outils d'analyse des vulnérabilités comme SATAN, ISS, Portscan et NMap;
   - les procédures de rapport et de résolution des incidents informatiques (p. ex. attaque par déni de service) et services--conseils internationaux en matière d'incidents informatiques;
   - les protocoles réseau comme HTTP, FTP et Telnet;
   - les protocoles de sécurité Internet comme SSL, S-HTTP, S-MIME, IPSec et SSH;
   - les protocoles TCP/IP, UDP, DNS, SMTP et SNMP;
   - les systèmes de détection des intrusions, les coupe-feux, les vérificateurs de contenu et les logiciels antivirus;
   - les infrastructures réseau comme les multiplexeurs, les routeurs/concentrateurs et les commutateurs.

b) Fournir du soutien pour l'analyse des incidents, notamment :
   - les mécanismes d'intervention;
   - la coordination de tous les plans de prévention et d'intervention;
   - les activités du Centre des opérations d'urgence (COE);
   - la coordination avec le Centre intégré d'évaluation des menaces et le Centre des opérations du gouvernement;
   - la participation au cadre de sécurité nationale intégré et à la stratégie nationale de cybersécurité.

c) Recueillir, compiler, analyser et diffuser de l'information publique sur les menaces et les vulnérabilités pesant sur les ordinateurs en réseau, les incidents de sécurité et les interventions en réponse aux incidents.

d) Mener des examens et des analyses des journaux de sécurité des systèmes sur site.

e) Produire des rapports sur les activités des systèmes et analyser des journaux et des incidents.

f) Contribuer à la gestion et à l'administration d'un centre de réponse aux incidents.

g) Réaliser les tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.

h) Préparer et fournir du matériel de formation adapté à la catégorie de ressources.

3.13.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins (10) ans d'expérience de la gestion des incidents.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b), c) et e) de la section 3.13.1.
O3	Compter au moins trois (3) années d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.14 Spécialiste de la conception de la sécurité des TI (Niveau 3)

3.14.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Examiner, analyser et appliquer : des méthodes, modèles et cadres d'architecture comme TOGAF, FEAP (gouvernement américain), BTEP (gouvernement canadien), GSRM, Zachman et UMM.
b) Examiner, analyser et appliquer un large éventail de technologies de sécurité, dont de nombreux types de systèmes, d'architectures et d'applications, et de nombreuses plateformes matérielles et logicielles, notamment :
    - les normes d'annuaire comme X.400, X.500 et SMTP;
    - les systèmes d'exploitation comme MS, Unix, Linux et Novell;
    - les protocoles réseau (HTTP, FTP et Telnet);
    - les routeurs, les multiplexeurs et les commutateurs réseau;
    - les protocoles DNS (services de nom de domaine) et NTP (protocole de synchronisation réseau).
c) Examiner, analyser et appliquer des architectures, des normes ainsi que des protocoles de communication et de sécurité de TI protégés (comme les protocoles IPSec, SSL, SSH, S-MIME et HTTPS).
d) Examiner, analyser et appliquer des protocoles de sécurité des TI pour toutes les couches de l'OSI (Interconnexion des systèmes ouverts) et toutes les piles TCP/IP (Transmission Control Protocol/Internet Protocol).
e) Examiner, analyser et appliquer l'importance et les conséquences des tendances du marché et de la technologie afin de les appliquer aux feuilles de route pour les architectures et la conception des solutions (p. ex. la sécurité des services Web, la gestion des incidents, la gestion des identités).
f) Examiner, analyser et appliquer des pratiques exemplaires et des normes en matière de zonage réseau et des principes de défense en profondeur.
g) Analyser les statistiques, les outils et les techniques de sécurité des TI.
h) Analyser les données de sécurité et présenter des avis et des rapports.
i) Préparer des rapports techniques, comme l'analyse des besoins, l'analyse des possibilités, les documents d'architecture technique, la modélisation mathématique des risques.
j) Informer les cadres supérieurs.
k) Assurer la conception d'architectures de sécurité et le soutien technique.
l) Réaliser des études liées à la classification ou à la désignation de sécurité des données.
m) Préparer des alertes et des avis de sécurité des TI sur mesure provenant de sources publiques et privées; réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.
n) Préparer et fournir du matériel de formation adapté à la catégorie de ressources.

3.14.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins (10) ans d'expérience en tant que spécialiste de la sécurité des TI.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b), c), d), e), f), g), l), m), n) de la section 3.14.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.15 Ingénieur en sécurité des TI (Niveau 3)

3.15.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Examiner, analyser et appliquer :
   - les normes d'annuaire comme X.400, X.500 et SMTP;
   - les systèmes d'exploitation comme MS, Unix, Linux et Novell;
   - les protocoles réseau comme HTTP, FTP et Telnet;
   - les notions de base des architectures sécurisées des TI, les normes et les protocoles de communications et de sécurité comme IPSec, IPv6, SSL et SSH;
   - les protocoles de sécurité des TI pour toutes les couches de l'OSI (interconnexion des systèmes ouverts) et toutes les piles TCP/IP;
   - le protocole de contrôle de transmission/protocole Internet;
   - les protocoles DNS (services de nom de domaine) et NTP (protocole de synchronisation réseau);
   - les routeurs, les multiplexeurs et les commutateurs réseau;
   - le renforcement de la sécurité des applications, des hôtes et du réseau, et meilleures pratiques de sécurité (p. ex. séquence de commandes en langage naturel [shell scripting], identification des services et contrôle des accès);
   - les systèmes de détection/prévention des intrusions, la défense contre les codes malveillants, l'intégrité des fichiers, la gestion de la sécurité d'entreprise et les coupe-feu;
   - les technologies sans fil;
   - les algorithmes cryptographiques.
b) Déceler les menaces techniques pesant sur les réseaux et leurs vulnérabilités.
c) Gérer la configuration de sécurité des TI.
d) Analyser les outils et les techniques de sécurité des TI.
e) Analyser les données de sécurité et présenter des avis et des rapports.
f) Analyser les statistiques sur la sécurité des TI.
g) Préparer des rapports techniques comme des plans d'analyse des options et de mise en œuvre de solutions de sécurité des TI.
h) Fournir un soutien pour la vérification et la validation par un tiers dans le cadre des projets de sécurité des TI, notamment :
   - la vérification de sécurité des TI, y compris les rapports, présentations et autres documents applicables;
   - l'examen des plans d'urgence, des plans de continuité des activités et des plans de reprise après sinistre;
   - la conception ou l'élaboration des essais et des exercices relatifs aux protocoles de sécurité des TI ainsi que leur réalisation;
   - la surveillance des projets.
i) Préparer et fournir du matériel de formation adapté à la catégorie de ressources.

3.15.2 Compétences obligatoires minimales

Nº	Description des critères
O1	Compter au moins dix (10) ans d'expérience en tant que spécialiste de la sécurité des TI.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b), c), e), f) et h) de la section 3.15.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.16 Spécialiste des analyses de vulnérabilité de la sécurité des TI (Niveau 3)

3.16.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Examiner, analyser et appliquer ce qui suit :
   - les outils d'analyse des agents de menace et autres nouvelles technologies, notamment les outils de protection des renseignements personnels, l'analyse prédictive, les techniques VoIP, la visualisation et la fusion des données, les dispositifs de sécurité sans fil, les PBX et les coupe-feu pour téléphonie;
   - les détecteurs d'accès entrant et les perceurs de mots de passe;
   - les services consultatifs publics en matière de vulnérabilité des TI;
   - les analyseurs de réseau et outils d'analyse des vulnérabilités comme SATAN, ISS, Portscan et NMap;
   - les protocoles réseau (HTTP, FTP et Telnet);
   - les protocoles de sécurité Internet, comme SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP,
   - la sécurité sans fil;
   - les systèmes de détection d'intrusion, les pare-feu et des vérificateurs de contenu;
   - les systèmes de détection et de prévention des intrusions dans les hôtes et les réseaux (gestion des antivirus).

b) Déceler les menaces pesant sur les réseaux et leurs vulnérabilités techniques.
c) Mener des examens et des analyses des journaux de sécurité des systèmes sur site.
d) Recueillir, compiler, analyser et diffuser de l'information publique sur les menaces et les vulnérabilités pesant sur les ordinateurs en réseau, les incidents de sécurité et les interventions en réponse aux incidents.
e) Préparer et tenir des réunions d'information sur les menaces, les vulnérabilités et les risques liés à la sécurité des TI.
f) Réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.
g) Préparer et fournir du matériel de formation adapté à la catégorie de ressources.

3.16.2 Compétences obligatoires minimales

Nº	Description des critères
O1	Compter au moins (10) ans d'expérience en tant que spécialiste des analyses de vulnérabilité de la sécurité des TI.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b), c) et d) de la section 3.16.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.17 Analyste de réseau (Niveau 3)

3.17.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Préparer des plans de mise en œuvre pour des technologies particulières.
b) Installer et surveiller des facettes particulières de la technologie.

c) Configurer et optimiser des installations techniques.
d) Faire du dépannage et trouver une solution aux problèmes des utilisateurs.
e) Se tenir informé des diverses technologies et des produits qui permettent de les prendre en charge.

3.17.2 Compétences obligatoires minimales

Nº	Description des critères
O1	Compter au moins (10) ans d'expérience en tant qu'analyste de réseau.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a) à e) de la section 3.17.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.18 Spécialiste du soutien des opérations (Niveau 3)

3.18.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Assurer l'administration des systèmes et le soutien aux opérations des systèmes, y compris la configuration des accès utilisateurs, des profils, des sauvegardes et des reprises ainsi que des opérations courantes des systèmes informatiques.
b) Effectuer les mises à niveau logicielles et apporter les correctifs.
c) S'entretenir avec le client afin d'assurer l'application des modifications exigées.
d) Surveiller les tendances de la charge de travail informatique et apporter des modifications afin d'assurer l'utilisation optimale des ressources informatiques.

3.18.2 Compétences obligatoires minimales

Nº	Description des critères
O1	Compter au moins (10) ans d'expérience en tant que spécialiste du soutien des opérations.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a) à d) de la section 3.18.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.19 Vérificateur de systèmes (Niveau 3)

3.19.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Examiner les politiques, les normes et les procédures organisationnelles des TI et offrir des conseils sur leur pertinence.
b) Passer en revue les systèmes en cours d'élaboration en examinant la documentation du projet, en effectuant des entrevues, en évaluant le travail accompli et, selon les constats, remettre des rapports sur la conformité aux politiques, aux normes et aux procédures ainsi que des rapports d'avancement.

c) Effectuer des examens de systèmes récemment mis en œuvre et remettre des rapports sur :
   - les avantages obtenus par rapport aux avantages prévus;
   - les caractéristiques livrées par rapport aux exigences énoncées;
   - la pertinence des contrôles et des caractéristiques de sécurité du système;
   - la satisfaction des utilisateurs évaluée à partir de sondages ou d'entrevues,
   - la performance et la fiabilité du système.
d) Effectuer des examens de systèmes en production depuis déjà quelque temps et remettre des rapports sur les problèmes, les lacunes et les irrégularités.

3.19.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins (10) ans d'expérience en tant que vérificateur de systèmes.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a) à d) de la section 3.19.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.20 Coordonnateur des essais (Niveau 3)

3.20.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Fournir des conseils et de l'orientation, et coordonner les efforts relatifs aux plans et stratégies d'essai, à la sélection d'outils d'essai automatisés et à la détermination des ressources requises pour les essais.
b) Planifier, organiser et inscrire au calendrier des activités d'essai pour des systèmes d'envergure, notamment l'exécution d'essais d'intégration des systèmes, d'essais spécialisés et d'essais d'acceptation par l'utilisateur (p. ex. essais marginaux).

3.20.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins (10) ans d'expérience en tant que coordonnateur des essais.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a) et b) de la section 3.20.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.21 Concepteur Web (Niveau 3)

3.21.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Définir l'architecture à utiliser dans les projets d'application Web.
b) Créer et appliquer des conceptions qui maximisent la convivialité des objets existants.

c) Effectuer la modélisation de l'architecture en vue de s'assurer que la conception cadre bien avec le travail déjà effectué.
d) Choisir le langage de réalisation de programme qui sera utilisé pour le projet.
e) Évaluer l'incidence des nouvelles exigences sur les applications Web existantes.
f) Élaborer le code en se fondant sur les documents relatifs à la conception et aux exigences.
g) Créer le code permettant les opérations d'écriture et de lecture dans la base de données.
h) Effectuer un essai unitaire du code avant de le soumettre aux essais d'intégration.
i) Surveiller la nécessiter de modifier la conception suivant la progression du projet.
j) Élaborer des plans de mise à l'essai du système.
k) S'assurer que les fonctionnalités ont été mises en œuvre selon les spécifications.
l) Définir les hypothèses et les contraintes touchant l'architecture en ce qui concerne la structure physique et la collecte de données.
m) Élaborer un plan afin de surveiller/vérifier la stabilité de la conception après la mise en œuvre.

3.21.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins (10) ans d'expérience en tant que concepteur Web.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), c), e), f), g), k), l) et m) de la section 3.2.1.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.22 Programmeur ou développeur de logiciels (Niveau 3)

3.22.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Élaborer et préparer des plans schématiques pour la résolution de problèmes opérationnels, scientifiques et techniques, à l'aide de systèmes informatiques complexes et de grande puissance.
b) Analyser les problèmes énoncés par les concepteurs ou analystes de systèmes à partir de facteurs comme le style et l'étendue des données à transférer depuis et vers les unités de stockage, la variété des éléments à traiter, la profondeur du tri et le format des résultats finaux imprimés.
c) Choisir et incorporer les programmes logiciels disponibles.
d) Concevoir dans le détail des programmes, des organigrammes et des diagrammes indiquant les calculs mathématiques et la séquence des opérations machine nécessaires pour copier et traiter les données et imprimer les résultats.
e) Traduire les graphiques d'acheminement détaillés en instructions machine codées et discuter de la planification des programmes avec le personnel technique.
f) Vérifier l'exactitude et l'intégralité des programmes en préparant des données d'échantillon et en les mettant à l'épreuve à l'aide d'essais de réception du système effectués par le personnel d'exploitation.

g) Corriger les erreurs de programmation en révisant les instructions ou en changeant la séquence des opérations.
h) Mettre à l'essai les instructions et rassembler les spécifications, les organigrammes, les diagrammes, les schémas de montage, les instructions de programmation et d'exploitation, afin de documenter les applications en vue de modifications ou de consultations ultérieures.

3.22.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins dix (10) ans d'expérience en tant que programmeur ou développeur de logiciels.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), b) et d) de la section 3.22.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.23 Architecte d'applications et de logiciels (Niveau 3)

3.23.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Élaborer des architectures, des stratégies et des cadres techniques, soit pour une organisation soit pour un secteur d'application important, afin de répondre aux besoins opérationnels et en matière d'applications.
b) Relever les politiques et les exigences qui excluent une solution en particulier.
c) Analyser et évaluer des solutions technologiques de rechange en vue de résoudre des problèmes opérationnels.
d) Veiller à l'intégration de tous les aspects des solutions technologiques.
e) Surveiller les tendances de l'industrie afin de s'assurer que les solutions respectent les orientations du gouvernement et de l'industrie en matière de technologie.
f) Analyser les exigences fonctionnelles afin de déterminer l'information, les procédures et les processus décisionnels.
g) Évaluer les procédures et méthodes en vigueur, définir puis consigner le contenu, la structure et les sous-systèmes applicatifs des bases de données, et préparer un dictionnaire de données.
h) Définir et décrire les interfaces entre les opérations manuelles et les opérations automatisées dans les sous-systèmes d'applications, ainsi qu'avec les systèmes externes et entre les nouveaux systèmes et les systèmes en place.
i) Définir les sources d'entrée et de sortie, y compris un plan détaillé pour la phase de conception technique et faire approuver le système proposé.
j) Déterminer et consigner les normes particulières aux systèmes qui s'appliquent à la programmation, à la documentation et aux essais et qui portent sur les bibliothèques de programmes, les dictionnaires de données, et les conventions d'appellation, entre autres choses.

3.23.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins dix (10) ans d'expérience en tant qu'architecte d'applications et de logiciels.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a), c), d), g) et i) de la section 3.23.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

3.24 Analyste de bases de données (Niveau 3)

3.24.1 Services requis

Les services requis peuvent comprendre notamment, mais non exclusivement, les suivants :

a) Définir de nouvelles structures de bases de données.
b) Définir une stratégie de conversion des données.
c) Définir les spécifications de conversion de base de données.
d) Produire la version finale de la stratégie de conversion.
e) Travailler en étroite collaboration avec les utilisateurs dans le but de tenir à jour et de protéger la base de données.
f) Définir les améliorations à apporter aux bases de données en place en établissant les besoins en information des utilisateurs et les exigences fonctionnelles et de performance du système.
g) Élaborer et mettre en œuvre les procédures qui assureront l'exactitude et l'exhaustivité des données stockées dans la base de données ainsi que la possibilité d'y accéder rapidement.
h) Servir de médiateur et résoudre les conflits en ce qui concerne les besoins des utilisateurs en matière de données.
i) Conseiller les programmeurs, les analystes et les utilisateurs sur l'utilisation efficace des données.

3.24.2 Compétences obligatoires minimales

N°	Description des critères
O1	Compter au moins dix (10) ans d'expérience en tant qu'analyste de bases de données.
O2	Compter au moins cinq (5) ans d'expérience, au cours des dix (10) dernières années, de l'exécution des responsabilités décrites aux points a) à i) de la section 3.24.1.
O3	Compter au moins trois (3) ans d'expérience, au cours des dix (10) dernières années, de l'élaboration de la prestation de services sur le Web.

PIÈCE JOINTE 1 DE LA PARTIE 4 – ÉVALUATION TECHNIQUE

1. APERÇU DE L'ÉVALUATION TECHNIQUE

La présente pièce jointe résume la méthode d'évaluation des propositions déposées à la suite de la demande de propositions (DP). La méthode d'évaluation est structurée de façon à assurer l'évaluation transparente et uniforme des propositions techniques des soumissionnaires. La proposition technique du soumissionnaire doit respecter chacun des critères obligatoires et chaque critère coté de manière suffisamment approfondie pour permettre à l'équipe d'évaluation d'évaluer sa conformité ou pour noter la réponse, s'il y a lieu, conformément aux critères énoncés. Par conséquent, le soumissionnaire doit fournir tout renseignement qu'il juge pertinent afin de faciliter l'évaluation de sa réponse relativement à une exigence précise. Aux fins de la présente évaluation, le soumissionnaire devrait assumer les calendriers prévus actuellement dans l'Annexe 2 de l'Annexe A.

Résumé de l'évaluation technique			
Nº	**Critère obligatoire**		**Satisfait/non satisfait**
O1	Projets de référence de l'entreprise : Restructuration des processus opérationnels et gestion du changement		
O2	Projets de référence de l'entreprise : Solution de TI		
O3	Références de client		
Nº	**Critères cotés**	**Pointage maximum**	**Note obtenue**
C1	Gestion du projet	620	
C2	Restructuration des processus opérationnels	360	
C3	Gestion des relations	160	
C4	Gestion de la sécurité	360	
C5	Migration des données de nature délicate	200	
C6	Plan de gestion du changement	380	
C7	Plan d'essai	160	
C8	Projets de référence de l'entreprise : Client du gouvernement du Canada	80	
C9	Projets de référence de l'entreprise : Gestion de cas, Microsoft Dynamics CRM et services vertical web initial destinées au public destinées au public	180	
	Pointage maximum pour les critères cotés	**2500**	
	Note de passage pour les critères cotés (70 %)	**1750**	

Remarque : *Consulter l'échelle générique d'évaluation technique figurant à la section 4 de la présente pour en savoir plus sur la méthode de notation des critères cotés.*

2. ÉVALUATION DE L'EXPÉRIENCE DES MEMBRES DE L'ÉQUIPE DU SOUMISSIONNAIRE

a. Pour les critères techniques obligatoires O1 et O2, de la section 3, Critères techniques obligatoires, et les critères cotés C8 et C9, de la section 4, Critères cotés, la définition de «soumissionnaire » en vertu de l'article 04 Définition de soumissionnaire des Instructions uniformisées 2003 est remplacée par la définition de soumissionnaire suivante :

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 comprend aussi la société mère, les filiales ou autres affiliées du soumissionnaire et ses sous-traitants.

b. Dans la présente demande de soumissions, un « Membre de l'Équipe » correspond à l'entité dont l'expérience est utilisée pour répondre aux critères d'évaluation O1, O2, C8 et C9. Lorsqu'un soumissionnaire cite l'expérience d'un Membre de l'Équipe, l'expérience acquise sera seulement prise en compte par le Canada si elle est accessible au soumissionnaire et si celui-ci peut compter sur l'expérience du Membre de l'Equipe et l'utiliser pendant l'exécution de tout contrat subséquent. Le soumissionnaire doit démontrer cette accessibilité au moyen de l'attestation fournie au tableau 5 du formulaire 1 de la partie 4 – formulaire de présentation de la demande de propositions. Si une expérience est présentée sans données à l'appui décrivant où, comment et par qui cette expérience a été acquise, ou à défaut d'indiquer clairement la présence de tout accord de partenariat conclu entre le soumissionnaire et le Membre de l'Équipe dont l'expérience est présentée aux fins d'évaluation, pourrait faire en sorte que l'expérience ne sera pas prise en compte dans l'évaluation. L'expérience présentée par le soumissionnaire pour répondre à des critères particuliers doit avoir été acquise dans le cadre de travaux dont le soumissionnaire, tel que défini dans 2.a. ci-dessus, était directement responsable.

3. CRITÈRES OBLIGATOIRES

Chaque soumission fera l'objet d'une évaluation visant à déterminer sa conformité aux critères obligatoires suivants. Les soumissions qui ne satisfont pas aux critères obligatoires seront déclarées irrecevables et ne seront pas considérées. Le soumissionnaire doit fournir les documents nécessaires à l'appui de sa conformité. Chaque critère obligatoire doit être évalué séparément. Aux fins de la présente évaluation, un projet est considéré comme ayant été réalisé avec succès lorsqu'une référence de client confirme que les services faisant l'objet du contrat ont été effectués selon les exigences de travail, le prix, le calendrier, le niveau de service et le rendement convenus d'un commun accord.

Nº	Exigence obligatoire	Renvoi à la proposition du soumissionnaire
O1	**Projets de référence de l'entreprise : Restructuration des processus opérationnels et gestion du changement** Le soumissionnaire doit citer **trois (3)** projets de référence en tout; **deux (2) des trois (3)** projets cités en référence doivent être semblables à ceux indiqués à l'ANNEXE A, sections 2 à 7. Tous les projets de référence doivent avoir été réalisés dans les **quinze (15)** années précédant la date de clôture des soumissions et avoir un volet d'échange de données avec le public sur Internet. Pour tous les projets de référence, le soumissionnaire a dû fournir des services portant notamment sur la restructuration des processus opérationnels et la gestion du changement pour un projet de transformation des systèmes opérationnels, et ce, à partir d'exigences	

opérationnelles générales et par l'intermédiaire d'une solution opérationnelle acceptée par le client.

Aux fins de la présente évaluation, un projet similaire serait défini comme ayant des exigences semblables à celles décrites aux parties 2 à 8 de l'annexe A, soit au moins 65 % du nombre total de comptes d'utilisateurs, de transactions et de types de transactions indiqués à la section 1, 3.1, Données volumétriques, de l'annexe A. Si la solution a été conçue et développée pour desservir un volume escompté d'utilisateurs, un nombre d'opérations et un éventail d'opérations qui répondent aux minimums indiqués dans le tableau ci-dessous, le projet peut être cité en référence. Il convient de noter que les volumes prévus doivent être demeurés supérieurs aux minimums indiqués tout au long de la durée du projet.

Paramètre	DP	Minimum pour les projets de référence
Comptes d'utilisateurs – internes et externes	184 392	119 854
Nombre de transactions	209 469	136 154
Types de transactions	12	7

A. Un (1) des trois (3) projets de référence devrait mettre l'accent sur les éléments suivants de la gestion du changement:
   i. Élaboration d'une approche de gestion du changement
   ii. Élaboration d'un plan de communication
   iii. Prestation de communication
   iv. Élaboration d'un plan de formation
   v. Prestation de la formation

B. Un (1) des trois (3) projets de référence devrait mettre l'accent sur les éléments de la restructuration des processus opérationnels:
   i. Élaboration d'un plan de réorganisation des processus opérationnels
   ii. Recommandation d'options pour l'optimisation des processus métier
   iii. Mise en œuvre du plan de restructuration des processus opérationnels

C. Au moins un (1) des projets cités en référence doit avoir été amorcé et achevé dans les cinq (5) ans précédant la date de clôture des soumissions et doit être semblable aux projets cités à l'ANNEXE, sections 2 à 7, comme il est indiqué ci-dessus.

Pour chaque référence, le soumissionnaire doit :

D. Fournir une description détaillée, comprenant entre autres :
   i. Un résumé;
   ii. Un énoncé du problème;
   iii. La stratégie de gestion du projet, qui comprend au minimum :
      a. La norme de l'industrie, la pratique exemplaire ou la méthode commerciale utilisée;

	b. La stratégie de mise en œuvre; c. La gestion des problèmes et des difficultés; d. La gestion des communications; e. L'atténuation des risques; f. Les technologies utilisées ou mises en œuvre; g. La gestion des ressources; h. La gestion du calendrier de projet (y compris l'échéancier du projet, du lancement à l'achèvement); iv. La gestion budgétaire (y compris le coût global des services faisant l'objet du contrat, à la fois au moment de l'attribution du contrat et à celui de la clôture du contrat); v. La description des utilisateurs; vi. Les données volumétriques, y compris le nombre de comptes d'utilisateurs, de transactions et de types de transactions; vii. Les différends contractuels et les problèmes de rendement.	
O2	**Projets de référence de l'entreprise : Solution de TI** Le soumissionnaire doit citer **trois (3)** projets de référence en tout; **deux (2) des trois (3)** projets cités en référence doivent être semblables à ceux indiqués à l'ANNEXE A, sections 2 à 7. Tous les projets de référence doivent avoir été réalisés dans les **quinze (15)** années précédant la date de clôture des soumissions et avoir un volet d'échange de données avec le public sur Internet. Pour tous les projets de référence, le soumissionnaire a dû fournir au minimum trois (3) des six (6) activités clés (services de conception, de configuration, de développement, de mise en œuvre, d'intégration et de migration des données liés à la TI). Les six (6) activités clés doivent avoir été un service contractuel dans le cadre d'au moins un projet de référence. Aux fins de la présente évaluation, un projet similaire serait défini comme ayant des exigences semblables à celles décrites aux parties 2 à 8 de l'annexe A, soit au moins 65 % du nombre total de comptes d'utilisateurs, de transactions et de types de transactions indiqués à la section 1, 3.1, Données volumétriques, de l'annexe A. Si la solution a été conçue et développée pour desservir un volume escompté d'utilisateurs, un nombre d'opérations et un éventail d'opérations qui répondent aux minimums indiqués dans le tableau ci-dessous, le projet peut être cité en référence. Il convient de noter que les volumes prévus doivent être demeurés supérieurs aux minimums indiqués tout au long de la durée du projet.	

Paramètre	DP	Minimum pour les projets de référence
Comptes d'utilisateurs – internes et externes	184 392	119 854
Nombre de transactions	209 469	136 154
Types de transactions	12	7

	Pour chaque référence, le soumissionnaire doit : A. Fournir une description détaillée, comprenant entre autres : i. Un résumé; ii. Un énoncé du problème; iii. La stratégie de gestion du projet, qui comprend au minimum : a. La norme de l'industrie, la pratique exemplaire ou la méthode commerciale utilisée; b. La stratégie de mise en œuvre; c. La gestion des problèmes et des difficultés; d. La gestion des communications; e. L'atténuation des risques; f. Les technologies utilisées ou mises en œuvre; g. La gestion des ressources; h. La gestion du calendrier de projet (y compris l'échéancier du projet, du lancement à l'achèvement); iv. La gestion du budget (y compris le coût global des services faisant l'objet du contrat); v. La description des utilisateurs; vi. Les données volumétriques, y compris le nombre de comptes d'utilisateurs, de transactions et de types de transactions; vii. Les différends contractuels et les problèmes de rendement. <u>En outre, le soumissionnaire doit démontrer que les exigences suivantes sont respectées dans l'ensemble des trois (3) projets de référence proposés.</u> B. La valeur des services professionnels fournis dans le cadre d'au moins un (1) projet cité en référence doit s'élever à 10 M$ ou plus ($ CA, taxes non comprises) pour un même contrat. Aux fins d'évaluation, le taux de change utilisé pour l'ajustement monétaire sera le taux de change moyen annuel publié par la Banque du Canada, en fonction de l'année d'attribution au soumissionnaire du contrat pour le projet de référence. C. Pour au moins un (1) projet de référence, les quatre (4) activités suivantes (services de conception, de mise en œuvre, d'intégration et de migration des données liés à la TI) et l'une des deux (2) activités suivantes : (configuration ou développement) doivent avoir été fournies dans le cadre d'un seul contrat. Le projet cité en référence doit être semblable à ceux indiqués à l'ANNEXE A, sections 2 à 7, comme défini ci-dessus. D. Au moins un (1) projet cité en référence doit avoir été présenté et terminé dans les cinq (5) années précédant la date de clôture des soumissions. E. Pour au moins un (1) projet de référence, le soumissionnaire a présenté une solution de services vertical web initial destinées au public mise en œuvre et intégrée à une solution dorsale de traitement aux fins d'échange d'information. La solution doit avoir fait l'objet d'exigences en matière de sécurité semblables à celles figurant à l'ANNEXE A, partie 5, section 1.2. Exigences relatives à la sécurité de la TI Aux fins de la présente évaluation, les exigences en matière de sécurité semblables désignent la mise en œuvre d'une solution utilisant des données de nature délicate (Protégé B) et nécessitent la protection de l'intégrité des données. Le projet de référence doit aussi être semblable à ceux figurant à l'ANNEXE A, sections 2 à 7, comme il est défini ci-dessus.	

O3	**Références de client** Pour chaque projet de référence présenté pour les critères O1 et O2, le soumissionnaire doit remplir le formulaire 2 de la partie 4. On pourrait communiquer avec la personne-ressource du client afin de valider les renseignements indiqués dans la réponse du soumissionnaire, conformément à la partie 4.2.4, Vérification des références.	

4. CRITÈRES COTÉS

Les soumissions qui satisfont tous les critères obligatoires seront évaluées et notées en fonction des critères qui figurent dans l'échelle générique et le tableau ci-dessous ainsi que dans la grille de pointage de la section 1 : Aperçu de l'évaluation technique. Les soumissions qui n'atteignent pas la note de passage pour les critères cotés seront déclarées irrecevables, et ne seront pas considérées. Le soumissionnaire doit fournir les documents nécessaires à l'appui de sa conformité. Chaque critère technique coté doit être évalué séparément. Le soumissionnaire retenu devra utiliser les procédures et méthodes décrites dans les divers documents demandés, qui serviront de base pour la prestation de la solution.

Échelle générique	
0 %	**Aucune réponse** – Le soumissionnaire n'a pas fourni de réponse ou les renseignements fournis par celui-ci ne se rapportaient pas au critère.
30 %	**Réponse partielle** – Les renseignements fournis ne satisfaisaient pas la plupart des exigences du critère coté ou présentaient d'importantes faiblesses. La soumission montre une faible compréhension des exigences de la demande de soumissions. L'approche proposée ne porte pas sur les facteurs importants et ne montre qu'un minimum de valeur technique et
60 %	**Réponse juste –** Les renseignements fournis remplissent certaines des exigences du critère coté, mais présentent de nombreuses faiblesses apparentes. La soumission montre une certaine compréhension des exigences de la demande de soumissions. L'approche proposée traite convenablement de certains des facteurs importants et présente une bonne valeur
80 %	**Réponse satisfaisante** – Les renseignements fournis satisfont très bien la plupart des exigences des critères cotés. La soumission montre une compréhension adéquate des exigences de la demande de soumissions. L'approche proposée présente seulement quelques faiblesses apparentes et fournit une excellente valeur technique et économique pour le
100 %	**Excellente réponse** – Les renseignements fournis satisfont très bien toutes les exigences des critères cotés. La soumission montre une compréhension profonde et complète des exigences de la demande de soumissions. L'approche proposée porte sur tous les facteurs importants, ne présente aucune faiblesse apparente et offre une excellente valeur technique et économique pour le Canada.

Pour chaque critère, les notes du soumissionnaire seront attribuées comme suit :
0 % – 0 % des points attribués à un critère
30 % – 30 % des points attribués à un critère
60 % – 60 % des points attribués à un critère
80 % – 80 % des points attribués à un critère
100 % – 100 % des points attribués à un critère

Par exemple, si une note de 80 % est accordée à une soumission pour l'évaluation du critère C1, alors la note accordée à la soumission pour ce critère sera calculée de la manière suivante :

Note pour le critère C1 :

Pointage maximal pour le critère C1 – Gestion du projet et mise en œuvre = 620 points

80 % x 620 points = 496 points

Nº	Critères cotés	Pointage maximal	Renvoi à la proposition du soumissionnaire
C1	**Gestion du projet** Le soumissionnaire devrait fournir un plan préliminaire de gestion du projet qui tient compte de la stratégie du soumissionnaire pour assurer la mise en œuvre des exigences décrites dans les sections 2 à 7, ANNEX A, en se servant du Système national de gestion de projet (SNGP). Le Canada évaluera le plan préliminaire de gestion du projet par le soumissionnaire, selon le degré auquel il satisfait les éléments demandés suivants et la façon dont il favorise l'atteinte des résultats escomptés et respecte les contraintes énumérées dans les sections 1 à 7, ANNEX A: A. **Gouvernance du projet et structure de l'équipe de projet**, y compris ce qui suit : i. Matrice des rôles et responsabilités, y compris les entités de l'entrepreneur et du gouvernement du Canada; ii. Description des relations et de la structure générale de l'équipe de projet (en précisant les groupes et les entités qui composent l'équipe de projet); iii. Diagramme du modèle de gouvernance qui sera utilisé par le soumissionnaire dans le cadre du projet. B. **Gestion de la portée des travaux** décrivant la gestion de la portée tout au long de l'étape de réalisation de projet. Cette description devrait porter sur ce qui suit : i. Un énoncé de la portée du projet décrivant la compréhension qu'a le soumissionnaire de la portée du projet, des principaux produits livrables et des critères d'acceptation proposés, ainsi que les contraintes et les hypothèses; ii. Une description de la gestion de la portée tout au long de l'étape de réalisation de projet. Cette description doit comprendre des renseignements sur les processus propres à la gestion de la portée, comme la vérification et le contrôle de la portée, ainsi que sur l'établissement de la structure de répartition	**Pointage maximum: 620** Pointage maximum de la partie A : 60 i. Pointage maximum : 20 ii. Pointage maximum : 20 iii. Pointage maximum : 20 Pointage maximum de la partie B : 140 i. Pointage maximum : 70 ii. Pointage maximum : 70	

	du travail (SRT), les rôles, les responsabilités, les outils, les techniques et l'établissement de rapports. C. **Gestion du calendrier** décrivant la stratégie du soumissionnaire pour la gestion des activités liées au projet de TSSI. La réponse devraitt indiquer notamment ce qui suit : i. Produits livrables connexes de chaque activité et de chaque jalon, incluant le chemin critique utilisé pour atteindre tel produit livrables; ii. Mesures d'atténuation et stratégies pour gérer les écarts de planification. D. **Calendrier de Plan** décrivant la stratégie du soumissionnaire pour la gestion des activités liées au projet de TSSI. La réponse devrait indiquer notamment ce qui suit : i. Dénomination de la structure de répartition du travail à deux niveaux [au minimum] (en plus du contexte du projet) : la structure de répartition du travail devrait indiquer tous les lots de travaux importants requis pour réaliser le projet; ii. Durée estimative de chaque activité, et dépendances (activités précédentes); Le calendrier de projet devrait être livré en format MS Project et tenir compte des contraintes indiquées dans ANNEX A. Le calendrier devrait respecter la date de début du 1er septembre 2017 et la date de lancement de la production du 31 mars 2019. E. **Gestion des risques** indiquant ce qui suit : i. Description du processus qui servira à cerner et à analyser les risques du projet, et à déterminer leur priorité; ii. Méthodes utilisées pour faire le suivi des risques, évaluer les changements relatifs à l'exposition à chaque risque, et s'adapter à ces changements; iii. Rôles et responsabilités en matière de gestion des risques; iv. Outils à utiliser pour la gestion des risques; v. Liste des cinq (5) principaux risques liés au projet et des stratégies d'atténuation proposées. F. **Gestion de la qualité** décrivant comment le soumissionnaire compte intégrer les critères entourant la qualité dans la gestion du projet et le développement des produits, des produits livrables et des processus. La réponse doit comporter ce qui suit :	Pointage maximum de la partie C : 80 i. Pointage maximum : 45 ii. Pointage maximum : 35 Pointage maximum de la partie D : 70 i. Pointage maximum : 35 ii. Pointage maximum : 35 Pointage maximum de la partie E : 150 i. Pointage maximum : 25 ii. Pointage maximum : 30 iii. Pointage maximum : 20 iv. Pointage maximum : 20 v. Pointage maximum : 50 Pointage maximum de la partie E : 120 i. Pointage maximum : 40	

	i. Description des processus de planification de la qualité, d'assurance de la qualité et de contrôle de la qualité; ii. Méthodes, outils et techniques de gestion de la qualité; iii. Rôles et responsabilités en matière de gestion de la qualité; iv. Définition d'une approche pour réagir au non-respect des critères de qualité.	ii. Pointage maximum : 30 iii. Pointage maximum : 30 iv. Pointage maximum : 20	
C2	**Restructuration des processus opérationnels** Le soumissionnaire devrait fournir une stratégie préliminaire de restructuration des processus opérationnels. Le Canada évaluera dans quelle mesure la stratégie préliminaire du soumissionnaire pour la restructuration des processus opérationnels offre les avantages établis au point 1.1 de la section 2 et démontre ce qui suit : A. Compréhension des processus opérationnels actuels du Secteur de la sécurité industrielle (SSI) et de la nécessité de recourir à des pratiques en matière de sécurité dans le cadre des diverses activités opérationnelles; B. Plan pour effectuer une analyse des écarts; C. Compréhension des contraintes et des répercussions; D. Quatre exemples d'occasions d'accroître l'efficacité et la rentabilité des processus et des approches de mise en œuvre proposées; E. Compréhension des risques et des possibilités aux fins d'atténuation et de résolution des risques; F. Planification des activités de restructuration des processus opérationnels.	**Pointage maximum : 360** Pointage maximum de la partie A : 60 Pointage maximum de la partie B : 50 Pointage maximum de la partie C : 40 Pointage maximum de la partie D : 60 (Maximum de 15 points pour chaque élément) Pointage maximum de la partie E : 50 Pointage maximum de la partie F : 100	
C3	**Gestion des relations** Le soumissionnaire devrait décrire l'approche qu'il adoptera à l'égard de la gestion des relations. Le Canada évaluera la mesure dans laquelle la réponse du soumissionnaire tient compte des éléments suivants : A. Approche globale à la gestion des relations relative au gouvernement du Canada et à l'intégrateur de systèmes. B. Communications entre le gouvernement du Canada et l'intégrateur de systèmes en ce qui a trait au modèle de gouvernance et à la structure de l'équipe proposés comme définis au point A du C1. A. C. Gestion et résolution de problèmes.	**Pointage maximum : 160** Pointage maximum de la partie A : 50 Pointage maximum de la partie B : 25 Pointage maximum de la partie C : 35	

	D. Planification mixte, approche à l'égard de la gestion du changement et établissement du calendrier de projet.	Pointage maximum de la partie D : 50	
C4	**Gestion de la sécurité** Le soumissionnaire devrait fournir, pour deux (2) scénarios opérationnels, une description des facteurs de sécurité nécessaires pour les activités à l'état stable, comme il est requis pour la solution de TSSI. La réponse devrait donner suffisamment de renseignements pour être considérée comme une description de bout en bout liée au scénario visé. Le document devrait mettre l'accent sur les exigences en matière de sécurité, comme elles sont indiquées dans la section réservée aux exigences en matière de sécurité de la partie 4 de l'annexe A. Le soumissionnaire devrait soumettre le document sur le concept des opérations de sécurité selon un format type utilisé dans l'industrie. GC ne fournira pas une table des matières. Aux fins de la présente évaluation, le scénario opérationnel se définit comme une seule activité ou un groupe d'activités connexes qui sont nécessaires à la réalisation d'un processus dans la solution. Chaque scénario utilisé dans cette réponse doit tenir compte de tous les contrôles de sécurité mentionnés aux points A, B, C et D ci-dessous. Voici des exemples de scénarios opérationnels : a) décrire le mouvement, de bout en bout d'un seul message au sein de Dynamics CRM vers un destinataire tiers; b) décrire un scénario dans le cadre duquel un inspecteur de TSSI sur le terrain mène une inspection sur place et présente le document définitif dans la solution reposant sur Dynamics CRM; c) décrire l'extraction, la transformation et le chargement des données aux fins de production d'un rapport d'aide à la décision; d) décrire le processus de délivrance des justificatifs d'identité d'un utilisateur; e) décrire la présentation d'une demande de services provenant d'un utilisateur (à l'exception du traitement TSSI); f) décrire le processus de transfert d'un dossier récemment achevé vers les archives de la « solution ». Même si la responsabilité de la mise en œuvre concrète de certaines des activités décrites pourrait incomber à un autre groupe au sein du gouvernement du Canada, le soumissionnaire devrait présumer, aux fins de la présente réponse seulement, qu'il sera responsable de	**Pointage maximum : 360** Pointage maximum de la partie A : 90 SC.47 a) Trois parties, 10 pts chaques SC.47 b) Quinze parties, 4 pts chaques Pointage maximum de la partie B : 120 SC.16 Trois parties, 40 pts chaques Pointage maximum de la partie C : 75 SC.9 a) Un partie, 75 pts Pointage maximum de la partie D : 75 SC.42 a) Un partie, 26 pts SC.42 b) Un partie, 25 pts SC.42 c) Quatre parties, 6 pts chaques	

	tous les aspects de la mise en œuvre des scénarios opérationnels de son choix. Il importe de traiter de tous les points, même ceux qui sont jugés non pertinents. Le soumissionnaire devrait expliquer son raisonnement quant aux points non pertinents. Le Canada évaluera dans quelle mesure l'approche du soumissionnaire à l'égard de la gestion de la sécurité tient compte des contrôles de sécurité requis. Plus particulièrement, l'approche devrait : A. faire référence à toutes les parties de la section SC.47 Généralités, et en traiter; B. faire référence à toutes les parties de la section SC.16 Architecture de sécurité de l'information, et en traiter; C. faire référence à toutes les parties de la section SC.09(a) Connexions au système d'information, et en traiter; D. faire référence à toutes les parties de la section SC.42 Plan d'essai de la sécurité, et en traiter.		
C5	**Migration des données de nature délicate** Selon son expérience précédente avec les projets d'intégration de technologies de l'information, le soumissionnaire devrait décrire son approche quant à l'exigence relative à la migration des données de la présente demande de soumissions. (Pour obtenir plus de détails sur les données, consultez l'annexe A, section 1, article 3.1.) Le Canada évaluera dans quelle mesure l'approche adoptée par le soumissionnaire démontre sa compréhension de l'activité de migration des données nécessaire dans le cadre du projet. Plus précisément, cette approche devrait tenir compte de ce qui suit : A. Une approche relative à la migration des données énumérant les activités clés à entreprendre; B. Les rôles, responsabilités et attentes définis du soumissionnaire et du Canada; C. Les risques et les stratégies d'atténuation précisément associés aux activités de migration; D. Les activités effectuées pendant la migration des données, qui permettront de satisfaire aux exigences en matière de sécurité de l'ITSG-33 se trouvant dans le tableau des exigences relatives à la sécurité, plus précisément : i. SC-21, Protection de l'information; ii. SC-23, Surveillance du système d'information; iii. SC-28, Récupération et reconstitution du système d'information; iv. SC-31, Validation de la saisie des données; v. SC-44, Sécurité – Généralités	**Pointage maximum : 200** Pointage maximum de la partie A : 70 Pointage maximum de la partie B : 40 Pointage maximum de la partie C : 40 Pointage maximum de la partie D : 50 (Maximum de 10 points pour chaque élément)	
C6	**Plan de gestion du changement** Le soumissionnaire devrait fournir un plan préliminaire de gestion des changements afin de décrire les méthodes, les approches, les	**Pointage maximum : 380**	

	outils et les ressources auxquels il aura recours pour répondre aux exigences en matière de gestion des changements de la présente demande de soumissions. Le Canada évaluera dans quelle mesure le plan préliminaire du soumissionnaire à l'égard de la gestion du changement appuie une transition efficace d'un état de départ vers un état ciblé, et démontre ce qui suit : A. Compréhension approfondie des exigences en matière de gestion du changement; B. Prise en considération des points suivants : i. Éviter l'interruption du service aux Canadiens; ii. Faciliter l'adoption du processus et la transition terminologique pour tous les utilisateurs des systèmes, y compris les utilisateurs externes et le personnel interne; iii. Garantir l'utilisation appropriée, conforme et rapide du nouveau système ainsi que l'entrée de données dans le nouveau système; et iv. Veiller à la qualité et à l'intégrité des services fournis. C. Méthode d'évaluation exhaustive pour évaluer l'efficacité des activités de gestion des changements.	Pointage maximum pour A : 100 Pointage maximum pour B : 200 i. Pointage maximum : 50 ii. Pointage maximum : 50 iii. Pointage maximum : 50 iv. Pointage maximum : 50 Pointage maximum pour C : 80	
C7	**Plan d'essai** Le soumissionnaire devrait fournir un plan d'essai préliminaire conformément aux exigences de l'ANNEXE A, section 6. Le soumissionnaire devrait se fonder sur les exigences opérationnelles et techniques, et l'architecture conceptuelle pour préparer un plan d'essai. Le Canada évaluera la mesure dans laquelle le plan d'essai du soumissionnaire démontre ce qui suit : A. Prise en considération des exigences en matière de sécurité du Plan d'essai de l'intégration de la sécurité, SC-42, ainsi que de la section 6 de l'ANNEXE A. B. Couverture adéquate des essais pour s'assurer que les exigences clés atteignent l'état de production nécessaire. Prise en considération des points suivants et renvoi à ces derniers : i. Essai d'intégration. ii. Essais fonctionnels et non fonctionnels, notamment les essais de sécurité. iii. Essais de migration des données. iv. Essai d'acceptation par le client. C. Détection et gestion des risques.	**Pointage maximum : 160** Pointage maximum pour A : 40 Pointage maximum pour B : 100 (Maximum de 25 points pour chaque élément) Pointage maximum pour C : 20	

C8	**Projets de référence de l'entreprise : Client du gouvernement du Canada** Le soumissionnaire devrait indiquer jusqu'à trois (3) projets de référence où il a livré avec succès une solution de TI pour un client du gouvernement du Canada. Les projets de référence peuvent inclure les projets cités en réponse aux critères obligatoires, s'il y a lieu. Le soumissionnaire devrait remplir le formulaire 2 jusqu'à la partie 4 pour tous les projets de référence cités en réponse à R8. Il est possible qu'on communique avec la personne-ressource du client afin de valider les renseignements indiqués dans la réponse du soumissionnaire, conformément à la partie 4.2.4, Vérification des références.	**Pointage maximum : 80** Un (1) projet cité en référence : 30 Deux (2) projets cités en référence : 50 Trois (3) projets cités en référence : 80	
C9	**Projets de référence de l'entreprise : Gestion de cas, Microsoft Dynamics CRM et services vertical web initial destinées au public** Le soumissionnaire devrait fournir jusqu'à trois (3) projets cités en référence qui seront évalués en fonction des éléments A, B et C ci-dessous. A. Les projets cités en référence ont fourni une solution nécessitant la conception et la configuration de TI, au moyen d'une solution de gestion de cas. B. Les projets cités en référence ont fourni une solution nécessitant la conception et la configuration de TI, au moyen de Microsoft Dynamics CRM 2015 (ou une version plus avancée) pour la solution. C. Les projets cités en référence ont fourni une solution nécessitant la conception, la configuration et l'intégration de la TI pour des services vertical web initial destinées au public, à des fins d'échange d'information avec Microsoft Dynamics 2015 ou une solution plus avancée. Aux fins de la présente évaluation, la gestion de cas se définit comme la gestion des activités, entre autres la mise au point, la coordination, la recherche, le soutien et l'exécution d'une demande de service d'un client, jusqu'à sa résolution. Les soumissionnaires sont invités à fournir des projets cités en référence qui sont en mesure de respecter les critères des points de l'évaluation afin de maximiser leur note. Les projets cités en référence peuvent inclure les projets indiqués afin de répondre aux critères obligatoires, s'il y a lieu. Le soumissionnaire devrait remplir le formulaire 2 de la partie 4 pour tous les projets cités en référence en réponse à C9. On pourrait communiquer avec la personne-ressource du client afin de valider les renseignements indiqués dans la réponse du soumissionnaire, conformément à la partie 4.2.4, Vérification des références.	**Pointage maximum : 180** Pointage maximum pour A : 60 Un (1) projet cité en référence : 40 Deux (2) projets cités en référence : 50 Trois (3) projets cités en référence : 60 Pointage maximum pour B : 60 Un (1) projet cité en référence : 40 Deux (2) projets cités en référence : 50 Trois (3) projets cités en référence : 60 Pointage maximum pour C : 60	

<table>
<tr>
<td></td>
<td>Par exemple, si un soumissionnaire fournit trois projets cités en référence où le critère A est respecté par les trois références, le critère B est respecté par deux des trois références et le critère C est respecté uniquement par une seule des trois références, le soumissionnaire recevrait alors un total de 150 points sur le maximum de 180 points pour le critère d'évaluation C9.
<table>
<tr><th>Référence</th><th>Critère A</th><th>Critère B</th><th>Critère C</th><th>Note totale C9</th></tr>
<tr><td>1</td><td>X</td><td>--</td><td>--</td><td rowspan="3"></td></tr>
<tr><td>2</td><td>X</td><td>X</td><td>--</td></tr>
<tr><td>3</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>Total des critères</td><td>60</td><td>50</td><td>40</td><td>150</td></tr>
</table>
</td>
<td>Un (1) projet cité en référence : 40

Deux (2) projets cités en référence : 50

Trois (3) projets cités en référence : 60</td>
<td></td>
</tr>
</table>

FORMULAIRE 3 DE LA PARTIE 4 – DEMANDE DE SOUMISSION – FORMULAIRE DE SOUMISSION FINANCIÈRE

FORMULAIRE 3 DE LA PARTIE 4
DEMANDE DE SOUMISSIONS – FORMULAIRE DE SOUMISSION FINANCIÈRE

1. <u>Soumission financière</u> :

1.1 Conformément à ce qui est indiqué à l'article 3.3 de la partie 3 de la demande de propositions, Instructions pour la préparation des soumissions de la section II, Soumission financière, la soumission financière du soumissionnaire doit comprendre le présent formulaire 3 de la partie 4, Demande de soumissions – Formulaire de soumission financière, dûment rempli.

1.2 Prix non indiqués : On demande aux soumissionnaires d'indiquer « 0,00 $ » pour tout article qu'il ne compte pas facturer ou qui fait déjà partie d'autres prix présentés dans les tableaux. Si le soumissionnaire n'indique pas le prix d'un article, un prix sera attribué aux fins d'évaluation seulement en fonction des renseignements suivants :
i. La moyenne sera calculée en fonction des prix proposés par tous les soumissionnaires ayant présenté une soumission recevable pour ce même article dont le prix n'a pas indiqué par le soumissionnaire.
ii. Un prix sera calculé aux fins d'évaluation selon la formule « moyenne plus 20 % », comme suit : On calcule tout d'abord la moyenne en saisissant le prix proposé par tous les soumissionnaires ayant présenté une soumission recevable pour ce même article dont le prix n'a pas indiqué par le soumissionnaire. On majore ensuite la moyenne de 20 % pour obtenir le prix « moyenne plus 20 % », qui servira à évaluer la soumission financière du soumissionnaire.
iii. Si le soumissionnaire est recommandé, le prix contractuel des articles touchés sera négocié avec le soumissionnaire avant l'attribution du contrat, et ce prix ne pourra pas dépasser le prix moyen calculé selon la formule décrite ci-dessus. Les prix négociés seront intégrés au barème de prix du contrat. Le Canada peut demander une justification des prix.

1.3 Le niveau d'effort estimatif précisé dans les colonnes B et E du tableau 2 est indiqué aux fins d'évaluation uniquement et ne figurera pas dans le barème de prix du contrat.

1.4 L'annexe B, Barème de prix sera élaborée en fonction des données saisies dans le présent formulaire par le soumissionnaire retenu.

2. Prix de lot ferme

2.1 En ce qui concerne l'exécution des travaux décrits aux sections 1 à 8 de l'ANNEXE A, Énoncé des travaux, le soumissionnaire doit proposer un prix de lot ferme et un calendrier des paiements d'étape conformément au TABLEAU 1 ci-dessous. Le prix de lot ferme total ne doit pas être inférieur à 6 000 000 $ ou supérieur à 11 000 000 $. Les tarifs doivent être en dollars canadiens, droits de douane inclus et taxes applicables en sus.

2.2 Le soumissionnaire doit tenir compte des points suivants dans la préparation de son calendrier des paiements d'étape :

2.2.1 Le prix de lot ferme total doit être ventilé en paiements d'étape, et le soumissionnaire doit proposer un calendrier pour ces paiements d'étape, lesquels doivent être versés à raison d'au plus une fois par mois. Les étapes du contrat doivent représenter des intervalles aussi réguliers que possible, et les éléments déclencheurs des paiements doivent être clairs. Le soumissionnaire peut présenter moins de 29 étapes, mais pas plus.

2.2.2 Les paiements d'étape doivent être conditionnels à la réalisation et à la livraison des travaux de l'étape ainsi qu'à l'acceptation de ces travaux par le responsable technique ou son représentant autorisé. Les étapes doivent être coordonnées avec la fourniture d'un livrable.

2.2.3 Le soumissionnaire doit présenter une description de chaque étape proposée, le montant du paiement d'étape et sa date d'échéance, exprimée en nombre de semaines ou de mois après l'attribution du contrat. La description devrait être suffisamment détaillée pour permettre au responsable technique de déterminer avec précision si l'étape a été accomplie. Le soumissionnaire doit détailler le niveau d'effort et les autres coûts connexes nécessaires à l'accomplissement de chacune des étapes. Le soumissionnaire doit passer en revue l'appendice 2 de l'annexe A, Étapes, et s'assurer que le calendrier des paiements d'étape proposé correspond aux étapes du projet.

2.2.4 La valeur du paiement lié à chacune des étapes doit être proportionnelle au niveau d'effort requis pour accomplir cette étape, et en aucun cas la valeur d'un paiement d'étape ne doit être si importante qu'elle constitue de fait un paiement anticipé (l'« attribution du contrat » n'est pas considérée comme une étape acceptable). Le Canada se réserve le droit de redistribuer le montant des étapes.

TABLEAU 1 – Prix de lot ferme et calendrier des paiements d'étape	**Sections 1 à 8 de l'annexe A, Énoncé des travaux *(aux fins de l'évaluation financière)***		
(A) Description de l'étape	**(B) Montant (en $ CA)**	**(C) Livrables de l'étape**	**(D) Date d'échéance**
1	$0.00		
2	$0.00		
3	$0.00		
…	$0.00		
29	$0.00		
(E) Prix de lot ferme total [somme de la colonne (B) pour toutes les étapes, de 1 à n]	**$0.00**		

3. Travaux sur demande :

L'entrepreneur doit proposer des tarifs journaliers fermes dans le tableau 2 pour les travaux sur demande effectués dans le cadre du contrat et de toute autorisation de tâches subséquente. Ces tarifs doivent englober le coût de la main-d'œuvre, les avantages sociaux, les frais d'administration, les frais généraux, l'estimation des travaux, les frais de déplacement, la marge bénéficiaire et les autres montants connexes, taxes applicables en sus. L'entrepreneur ne peut pas facturer de tarifs journaliers pour la préparation de l'estimation des travaux ou des autorisations de tâches. Les tarifs doivent être en dollars canadiens, droits de douane inclus et taxes applicables en sus.

Tableau 2	**Travaux sur demande (article 9 de l'ANNEXE A, Énoncé des travaux) – Autorisation de Tâches – Catégories de ressources (aux fins de l'évaluation financière)**						
Catégories de ressources	**(A)** Tarif journalier ferme tout compris pour la période initiale du contrat	**(B)** Niveau d'effort (NE) estimatif pour la colonne (A)	**(C) Sous-total (A × B)**	**(D)** Tarif journalier ferme tout compris pour les périodes d'option	**(E)** NE estimatif pour la colonne (D)	**(F) Sous-total (D × E)**	**(G) Coux total estimatif par catégorie de ressources [C + F]**
1. Expert-conseil en communications (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
2. Développeur de didacticiel (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
3. Spécialiste en conversion de données (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00
4. Administrateur de bases de données (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00
5. Modélisateur de données (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00
6. Architecte en Gestion Information (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00
7. Programmeur / Analyste (Niveau 3) – Business Objects	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
8. Programmeur / Analyste (Niveau3) – MS Dynamics CRM	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
9. Développeur de page Web (Niveau 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
10. Expert-conseil en restructuration des processus opérationnels (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00

Tableau 2	**Travaux sur demande (article 9 de l'ANNEXE A, Énoncé des travaux) – Autorisation de Tâches – Catégories de ressources (aux fins de l'évaluation financière)**						
Catégories de ressources	**(A)** Tarif journalier ferme tout compris pour la période initiale du contrat	**(B)** Niveau d'effort (NE) estimatif pour la colonne (A)	**(C) Sous-total (A × B)**	**(D)** Tarif journalier ferme tout compris pour les périodes d'option	**(E)** NE estimatif pour la colonne (D)	**(F) Sous-total (D × E)**	**(G) Coux total estimatif par catégorie de ressources [C + F]**
11. Expert-conseil en gestion du changement (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
12. Spécialiste de la cybersécurité (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00
13. Spécialiste de la gestion des incidents (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
14. Spécialiste de la conception de la sécurité des TI (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
15. Ingénieur en sécurité des TI (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
16. Spécialiste des analyses de vulnérabilité de la sécurité des TI (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
17. Analyste de réseau (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00
18. Spécialiste du soutien des opérations (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
19. Vérificateur de systèmes (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
20. Coordonnateur des essais (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
21. Concepteur Web (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
22. Programmeur ou développeur de logiciels (Niveau 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
23. Architecte d'applications et de logiciels (Niveau 3)	$0.00	40	$0.00	$0.00	80	$0.00	$0.00
24. Analyste de bases de données (Niveau 3)	$0.00	80	$0.00	$0.00	40	$0.00	$0.00
	(H) Coût total estimatif [somme de la colonne (G) pour toutes les catégories de ressources]						**$0.00**

4. Prix total évalué de la soumission

Voici le mode de calcul du prix total évalué de la soumission :	
Prix total évalué réel de la soumission :	$0

Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Better government: with partners, for Canadians

Solutions technologiques d'authentification électronique

Architecture et spécifications de l'interface

Version 2.0 :

Profil de mise en place

État: Version de base pour la DP nº 3
Version définitive 7.2
Date de modification: le 25 mars, 2011 13:57
Nom du fichier: CA - CATS IA&S V2 0_Deployment Profile_Final r7.2_fr.doc

Pour obtenir de plus amples renseignements, veuillez communiquer avec:
Bob Sunday
Programme d'authentification électronique
Direction du dirigeant principal de l'information
Secrétariat du Conseil du Trésor
613-941-4764
Courriel : robert.sunday@tbs-sct.gc.ca

Approbation par : SCT, CDPI

Comité des DG sur l'authentification électronique

Canada

Fiche des révisions

N° de VERSION	DESCRIPTION	DATE DE DISTRIBUTION	État	AUTORISATION ET NOTES
0.1	Texte initial	17 septembre 2010	Première version – travail en cours	Bob Sunday, SCT
0.2	Version préliminaire à examiner en vue d'une approbation durant l'atelier de l'équipe corsaire de la DP nº 3 (28 octobre)	4 octobre 2010	Version préliminaire définitive	Bob Sunday, SCT
version 4	Document recommandé en vue d'une approbation par les responsables de la gouvernance à titre de document de base	15 novembre 2010	Version de base recommandée	Bob Sunday, SCT Avec beaucoup d'aide des membres de l'équipe d'élite de la DP no 3 et de leurs collègues
version 5	Document de base recommandé pour approbation par le Comité des DG sur l'authentification électronique	19 novembre 2010	Version de base recommandée	Bob Sunday, SCT
version 6 (finale)	Document de base définitif à joindre à l'ébauche de DP n° 3	25 novembre 2010	Version de base pour la DP n° 3	Bob Sunday, SCT
version 7 (finale)	Document de base définitif à joindre à l'ébauche de DP n° 3	14 decembre 2010	Version de base pour la DP n° 3	Bob Sunday, SCT
Ébauche r7.1	Document de base (avec mises à jour proposées) à joindre à la DP n° 3 finale	9 février 2011	Version de base pour la DP n° 3	Bob Sunday, SCT
version 7.2 (finale)	Document de base à joindre à la DP n° 3 finale	25 mars 2011	Version de base pour la DP n° 3	Bob Sunday, SCT

Avant-propos

Note concernant la présente version – ébauche r7.2

Le présent document, « *Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de mise en place* » constitue la version de base actualisée du document « *Architecture et spécifications de l'interface de la Solution tactique d'authentification électronique (STAE)* ». La présente version constitue le document de base officiel approuvé par le Comité des DG sur l'authentification électronique en vue d'une distribution avec la DP n° 3.

Les changements apportés par la suite au présent document de base seront traités en même temps que les clauses et demandes officielles de changement.

Table des matières

1 Introduction

1.1 Programme d'authentification électronique – Vision

La vision du Programme d'authentification électronique du gouvernement du Canada est partiellement illustrée ci-dessous.

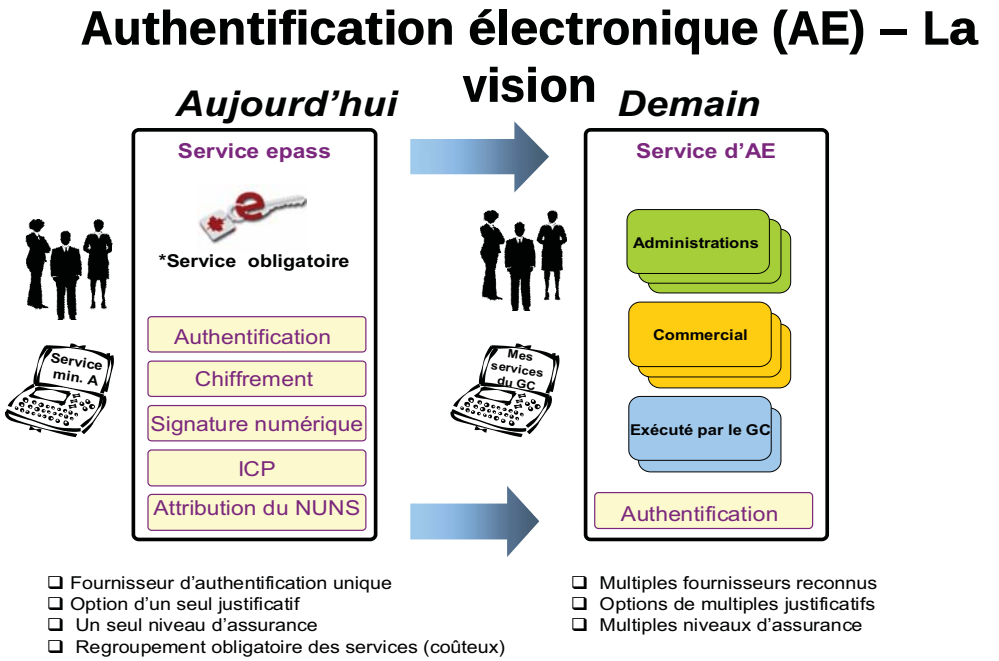


Figure 1 : Vision de l'authentification électronique

1.2 Vue d'ensemble du Profil de mise en place de l'ASI des STAE

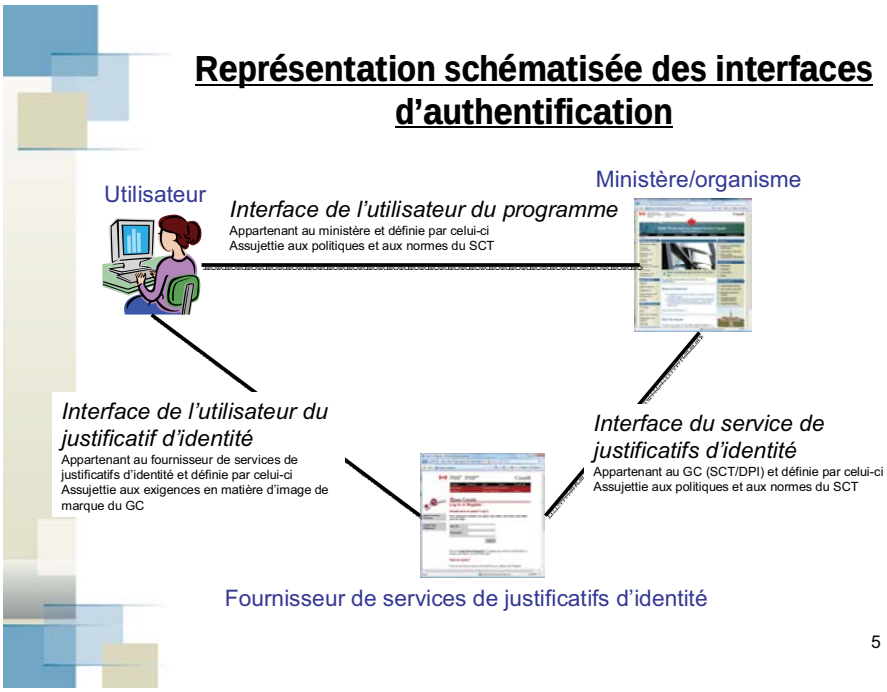


Figure 2 : Représentation schématisée des interfaces d'authentification

Le présent « *Profil de mise en place de l'ASI des STAE* » [ASI STAE 2] est un profil de mise en place qui vise une participation à l'environnement d'authentification électronique du gouvernement du Canada. Il décrit l'interface de messagerie « Interface du service de justificatifs d'identité » qui est précisée à la figure 2, Représentation schématisée des interfaces d'authentification.

Il porte sur les services configurés pour participer à titre de fournisseurs de services et de fournisseurs de services de justificatifs d'identité (FSJ). Au sein du gouvernement du Canada, les fournisseurs de services sont également appelés parties utilisatrices (PU) (il s'agit en général de services ministériels en ligne), tandis que les fournisseurs d'identificateurs sont appelés fournisseurs de services de justificatifs d'identité (FSJ). Le GC utilise également le terme courtier de justificatifs d'identité (CJI), qui est une entité de système qui agit à la fois comme fournisseur de services de justificatifs d'identité pour les PU et en tant que PU lorsqu'il communique avec les fournisseurs de services de justificatifs d'identité connexes. Dans ces situations, la documentation du SAML utilise le terme Mise en cache du fournisseur de services de justificatifs d'identité.

NOTA : Dans le présent document, nous employons les termes « fournisseurs de services » et « fournisseurs de services de justificatifs d'identité ». D'autres documents sur l'authentification électronique emploient également les termes parties utilisatrices et fournisseurs de services de justificatifs d'identité. La documentation du SAML (langage de balisage des déclarations de sécurité) et de l'initiative Kantara utilise les termes « fournisseurs de services » et « fournisseurs d'identificateurs ». Nous n'utilisons pas le terme courtier de justificatifs d'identité (CJI) dans le présent document, du fait qu'il s'agit d'une combinaison des rôles de fournisseur de services et de fournisseur de services de justificatifs d'identité.

Le Profil de mise en place est une version peaufinée de l'ancien document du gouvernement « *Architecture de l'interface et spécification de la solution tactique d'authentification électronique (STAE)* » [ASI STAE 1]

Ce profil n'est pas un tutoriel ni un document d'orientation. L'OGFJGC pourra proposer d'autres directives et des cas d'utilisation.

1.3 Conformité avec le Profil de mise en place de l'ASI des STAE

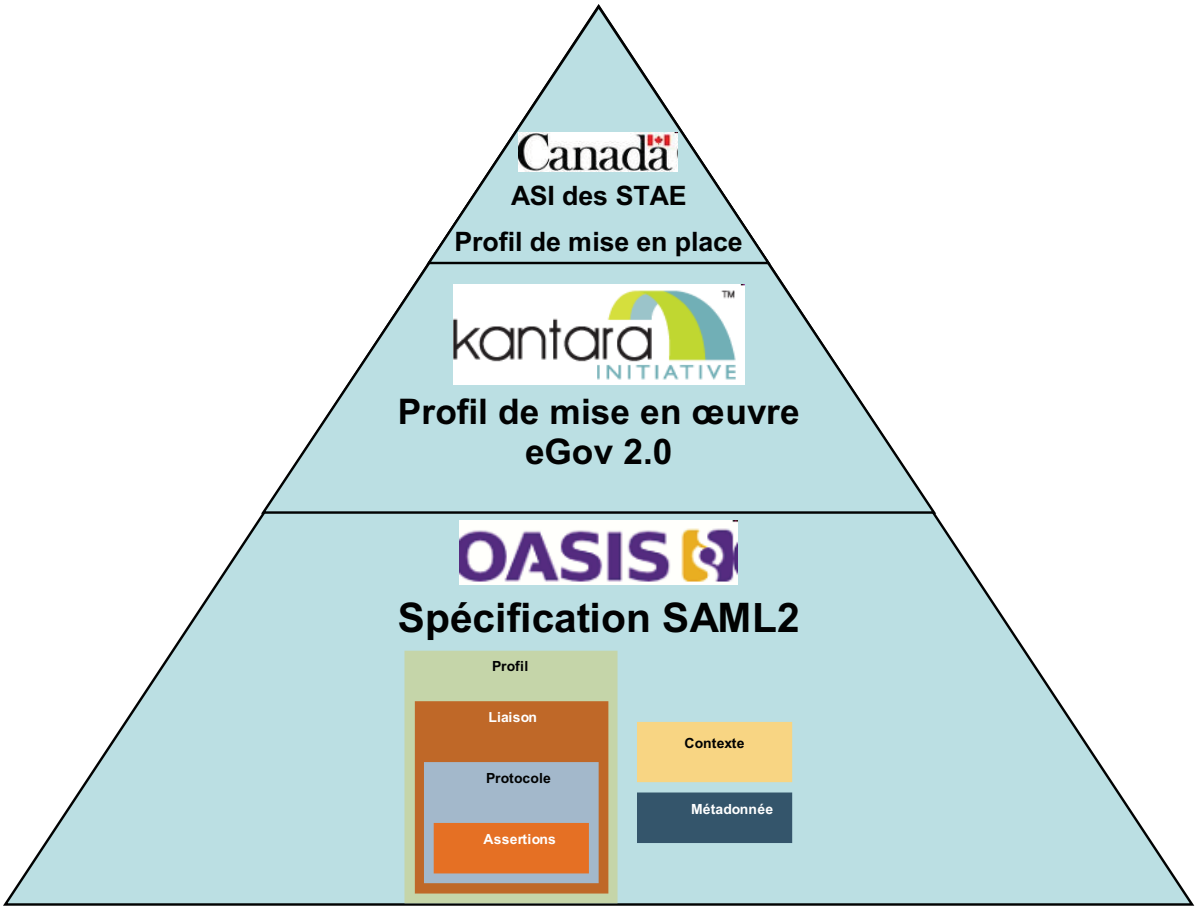


Figure 3 : Modules de l'architecture de l'interface de l'authentification électronique

Le Profil de mise en place est fondé sur le Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, sans toutefois lui être parfaitement conforme. Les exigences normatives du présent Profil de mise en place du gouvernement qui touchent les sections pertinentes du Profil eGov 2.0 sont décrites à la section 2 du présent document. Le Profil eGov 2.0 se fonde sur les spécifications SAML 2.0 élaborées par le Security Services Technical Committee (SSTC) d'OASIS, mais restreint les caractéristiques, éléments, attributs et autres valeurs de base de SAML 2.0 exigées pour les fédérations et les mises en place du gouvernement électronique. Les actions et les caractéristiques SAML respectent celles des spécifications OASIS SAML 2.0 [SAML2*], sauf indication contraire.

NOTA : Les essais d'interopérabilité réalisés par des organismes externes, comme l'initiative Kantara, peuvent aider à vérifier la conformité. Ainsi, les acquisitions du gouvernement qui doivent être conformes au présent Profil de mise en place peuvent également exiger que les logiciels sous-jacents respectent les essais d'interopérabilité extérieurs.

Toutefois, ces essais extérieurs ne constituent pas une vérification complète et définitive de la conformité avec les exigences de mise en place du gouvernement. D'autres essais peuvent ainsi être exigés par l'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) en vue d'une participation à la FJGC.

1.3.1 Notation

Cette spécification utilise du texte normatif pour décrire les capacités en SAML.

Dans ce contexte, il faut interpréter les mots clés « MUST », « MUST NOT », « REQUIRED », « SHALL », « SHALL NOT », « SHOULD », « SHOULD NOT », « RECOMMENDED » « MAY » et « OPTIONAL » de la manière décrite dans le document [RFC2119] :

> …il FAUT les utiliser seulement lorsqu'ils sont nécessaires à des fins d'interopérabilité ou pour limiter les opérations qui risquent du causer du tort (p. ex., en limitant les retransmissions)…

Ces mots clés sont donc écrits en majuscules lorsqu'ils doivent servir à spécifier de façon non ambiguë des exigences au-delà des protocoles et touchant des fonctions des applications et opérations qui affectent l'interopérabilité et la sécurité des applications.

1.4 Changements par rapport à l'*Architecture de l'interface et spécification de la STAE1*

Le présent document diffère du document [ASI STAE 1] à plusieurs égards :

1.4.1 Priorité à la mise en place plutôt qu'à la technologie sous-jacente
1.4.2 Prise en charge explicite du niveau d'assurance exigée
1.4.3 Envoi OBLIGATOIRE des réponses d'authentification
1.4.4 Mise en œuvre OBLIGATOIRE du profil de dépistage des fournisseurs de services de justificatifs d'identité
1.4.5 Utilisation des demandes de canal d'appui pour la fermeture de session unique

Ces changements sont décrits de façon générale ci-après. Pour connaître tous les détails de la conformité normative imposée au présent Profil de mise en place, reportez-vous à la section 2 du présent document, « Exigences (normatives) de la mise en place ».

1.4.1 Priorité à la mise en place plutôt qu'à la technologie sous-jacente

Le présent document du Profil de mise en place assouplit les règles, mais pas les exigences liées à la conformité, qui stipulaient auparavant que les logiciels sous-jacents des fournisseurs de services et des fournisseurs de services de justificatifs d'identité réussissent les essais d'interopérabilité.

Les nouvelles règles vont exiger la mise en place du « service » du fournisseur de services de justificatifs d'identité et du fournisseur de services en vue des essais d'interopérabilité et d'une certification en fonction des règles précisées dans le présent document de Profil de mise en place.

Les documents du plan d'essai de l'initiative Kantara indiquent de nombreux jeux d'essais avec lesquels on peut vérifier de nombreuses sections du présent Profil de mise en place; ils aideront grandement la FJGC à établir la conformité. En outre, le fait d'utiliser des logiciels commerciaux ayant réussi les essais d'interopérabilité de la Liberty Alliance ou de l'initiative Kantara augmente beaucoup les chances de respecter adéquatement les exigences de mise en place établies.

Il découle de cette réorientation que l'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) devient l'organisme autorisé à déterminer si une mise en place (fournisseur de services ou fournisseur de services de justificatifs d'identité) a fait l'objet d'essais suffisants pour que le service en question fasse partie de la fédération.

1.4.2 Prise en charge explicite du niveau d'assurance exigée

Le FJGC appuie plusieurs niveaux d'assurance et, ainsi, on doit préciser le niveau souhaité (pour le fournisseur de services) et le niveau fourni (par le fournisseur de services de justificatifs d'identité). Le soutien du niveau d'assurance est exigé conformément au document [SAML2 Assurance]. Les niveaux d'assurances d'authentification électronique du gouvernement du Canada sont décrits dans le document [ITSG-31] et les URI correspondants sont précisés dans le présent « *Profil de mise en place de l'ASI des STAE* », à la section 2.4.2, Niveaux d'assurance de l'authentification électronique du gouvernement du Canada.

Les fournisseurs de services doivent demander un niveau d'assurance du gouvernement du Canada précis avec l'opérateur de comparaison « exact ». Précisons que le fournisseur peut indiquer que plus d'un niveau d'assurance est acceptable. Une situation de la sorte peut s'avérer utile dans les cas où le niveau 2 est requis, mais si le fournisseur de services est disposé à accepter (et peut-être à payer les frais correspondants) au niveau 3 si le niveau 2 n'est pas réalisable.

Il faut configurer les fournisseurs de services de justificatifs d'identité pour les faire correspondre au(x) niveau(x) d'assurance exact(s) pour lesquels ils sont certifiés. Les fournisseurs de services de justificatifs d'identité doivent rejeter toute demande d'authentification d'un niveau d'assurance pour lequel ils n'ont pas été certifiés en précisant le codé d'état approprié. Les fournisseurs de services de justificatifs d'identité doivent fournir le niveau d'assurance précis demandé.

Les exigences visant les métadonnées portent notamment sur la prise en charge additionnelle du niveau d'assurance, conformément aux détails du document [SAML2 Assurance].

1.4.3 Envoi OBLIGATOIRE des réponses d'authentification

Les produits commerciaux existants diffèrent sur le plan de la capacité à envoyer des réponses d'authentification dans certains cas, pendant le traitement de la demande d'authentification. Dans le STAE1, l'utilisateur se butait alors à un problème (par exemple, l'utilisateur pouvait annuler l'ouverture de session).

Le Profil eGov 2.0 [eGov 2.0] de l'initiative Kantara exige désormais qu'on produise et envoie les réponses, que la demande d'authentification réussisse ou non. Cette exigence est également précisée par le présent « *Profil de mise en place de l'ASI des STAE* », et elle favorisera l'amélioration de la messagerie utilisateur et une meilleure continuité du dialogue des utilisateurs.

1.4.4 Mise en œuvre OBLIGATOIRE du profil de dépistage des fournisseurs de services de justificatifs d'identité

Dans un environnement à un seul fournisseur de services de justificatifs d'identité, il n'était pas nécessaire d'indiquer le fournisseur auquel l'utilisateur souhaitait faire appel. Ainsi, l'exigence de la STAE1 pour le profil de dépistage, qui permet à l'utilisateur de choisir son fournisseur de services de justificatifs d'identité, a été reportée pour les fournisseurs de services et les fournisseurs de services de justificatifs d'identité.

L'environnement du gouvernement du Canada, qui appuie désormais plusieurs fournisseurs de services de justificatifs d'identité, exige donc un mécanisme de prise en charge du choix du fournisseur de services par l'utilisateur et le fournisseur de services de justificatifs d'identité.

Le présent « *Profil de mise en place de l'ASI des STAE* » ne modifie pas la spécification du document [ASI STAE 1], mais il exige désormais l'inclusion dans la mise en place du profil de dépistage du fournisseur de services de justificatifs d'identité. Il se peut donc que les fournisseurs de services et les fournisseurs de services de justificatifs d'identité existants doivent modifier leurs services en conséquence.

1.4.5 Utilisation des demandes de canal d'appui pour la fermeture de session unique

Les installations existantes appuient la fermeture de session unique à l'aide des liaisons de canal d'avant-plan SAML, qui font communiquer le navigateur de l'utilisateur tour à tour avec chaque fournisseur de services. En d'autres termes, les fermetures de session de chaque fournisseur de services sont effectuées successivement, ce qui augmente les risques qu'une erreur laisse l'utilisateur dans un état indéterminé.

Pour améliorer cette situation, la STAE2 ajoute l'appui des liaisons de canal d'appui, afin de prendre en charge la fermeture de session unique, et elle empêche la propagation des fermetures de session en avant-plan vers les autres PU touchées. Les liaisons SOAP sont ainsi prises en charge pour les demandes et les réponses de fermeture de session, conformément aux spécifications du Profil eGov 2.0 [eGov 2.0].

Le ministère peut donc maintenant :

- garder le contrôle de la session de l'utilisateur et indiquer au fournisseur de services de justificatifs d'identité de fermer la session; ou
- laisser au fournisseur de services de justificatifs d'identité le contrôle de la session de l'utilisateur,
    - afin de permettre au fournisseur de services de justificatifs d'identité d'informer l'utilisateur au sujet d'erreurs précises pouvant survenir et, à la fin de la session, de rediriger l'utilisateur au fournisseur de services.

1.4.6 Utilisation du témoin (cookie) de langue du gouvernement pour communiquer la langue

La *Loi sur les langues officielles* (LLO) du gouvernement du Canada et la Politique sur la Normalisation des sites Internet stipulent l'utilisation systématique d'un moyen de communication de la préférence de langue de l'utilisateur, même si l'authentification échoue et qu'aucune assertion n'est produite.

La STAE1 n'a prévu aucun mécanisme de transmission au fournisseur de services de la langue de l'utilisateur. La clé d'accès du gouvernement devait ainsi présenter une première page bilingue et il était alors impossible de communiquer un changement de langue en cas d'échec de l'authentification, ce qui n'était pas entièrement conforme aux exigences de la LLO.

La STAE2 prévoit plutôt pour l'authentification électronique l'utilisation d'un témoin de langue du gouvernement. Ce témoin lié à la session est mis à jour et lu par les fournisseurs de services et les fournisseurs de services de justificatifs d'identité s'il leur faut connaître la langue de l'utilisateur, afin de respecter les exigences de la LLO.

Nota : Bien que cette fonction soit nécessaire pour l'authentification électronique, son utilisation s'applique aussi à d'autres situations propres au gouvernement, comme les portails. Afin qu'elle puisse être adjointe à une norme gouvernementale future plus pertinente, elle a été définie de façon générique et présentée dans une annexe du présent document.

1.4.7 Avis de révocation d'un justificatif d'identité

La STAE1 ne prévoyait aucun mécanisme d'avis à un ministère si un fournisseur de services de justificatifs d'identité annulait un justificatif d'identité utilisé au sein de ce ministère. Or, plusieurs ministères ont besoin d'une telle fonction afin de mieux gérer leurs effectifs.

La STAE2 prévoit la prise en charge par les fournisseurs de services de justificatifs d'identité de l'envoi de ces données par demandes de canal d'appui, à l'aide du protocole, et du profil, de gestion d'identificateurs de nom SAML.

Ces améliorations permettent aux fournisseurs de services d'indiquer à l'aide de métadonnées qu'ils souhaitent recevoir ces messages, et le GC peut aussi exiger des fournisseurs de services de justificatifs d'identité qu'ils avisent un fournisseur de services en cas d'annulation d'un justificatif d'identité utilisé auparavant par ce fournisseur de services. Les fournisseurs de services de justificatifs d'identité ne doivent informer un fournisseur de services de l'annulation d'un code d'utilisateur que s'ils ont déjà transmis des assertions à ce fournisseur pour l'utilisateur visé.

1.4.8 Corrections et mises à jour diverses

Différentes corrections et mises à jour doivent être effectuées :

- Afin de traiter correctement les IAP envoyés à plusieurs ministères, l'identificateur de nom (`<NameID>`) qui figure dans l'assertion peut comprendre le qualificatif de nom du fournisseur de service (`SPNameQualifier`), ce qui corrige un bogue de la STAE1.
- Toutes les fermetures de session sont globales. Ainsi, toute fermeture entraîne la transmission d'un profil complet de fermeture de session unique à tous les fournisseurs de services qui prennent part à la session de l'utilisateur. Le fournisseur de services de justificatifs d'identité ou le fournisseur de services n'aura plus à demander le choix entre une fermeture de session locale et une fermeture globale, ce qui règle un problème de convivialité.
- L'indication `RelayState` ne doit pas être transmise dans les messages de réponse d'authentification, sauf si elle a été reçue dans le message correspondant de demande d'authentification. Cela règle un bogue de la STAE1.
- L'indication `SessionNotOnOrAfter` ne doit pas être transmise dans les messages de réponse d'authentification électronique, ce qui permet au fournisseur de services d'établir lui-même le délai de temporisation. Cela règle un problème de convivialité.
- La signature graphique du fournisseur de services et le nom à afficher sont ajoutés aux métadonnées du fournisseur de services. La STAE2 peut ainsi respecter d'éventuelles exigences en matière d'association de marques.

1.5 Documents de référence

[ASI STAE 1]	« Architecture de l'interface et spécification de la Solution tactique d'authentification électronique (STAE) Version 1.0 », 23 janvier 2009.
[ASI STAE 2]	« Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 : Profil de mise en place »; le présent document.
[eGov 2.0]	« Kantara Initiative eGovernment Implementation Profile of SAML V2.0 » (initiative Kantara, version 2.0 du profil de mise en œuvre du gouvernement électronique SAML 2.0) : http://kantarainitiative.org/confluence/download/attachments/42139782/kantara-egov-saml2-profile-2.0.pdf
[ITSG-31]	« Conseils en matière de sécurité des TI (ITSG), Guide sur l'authentification des utilisateurs pour les systèmes TI », publié par le

	Centre de la sécurité des télécommunications Canada; consultable à l'adresse suivante : http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-fra.html
[RFC 1766]	Tags for the Identification of Languages (Balises pour la désignation des langues) http://www.ietf.org/rfc/rfc1766.txt
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels (Mots clés à utiliser dans les documents pour indiquer les niveaux d'exigences) http://www.ietf.org/rfc/rfc2119.txt
[SAML2 *]	Tous les documents de référence SAML2 sont offerts à l'adresse suivante : http://docs.oasis-open.org/security/saml/v2.0 ainsi qu'à cette adresse : http://wiki.oasis-open.org/security/FrontPage
[SAML2 Assurance]	OASIS Committee Specification 01, SAML V2.0 Identity Assurance Profiles Version 1.0, novembre 2010. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf [SAML2 Liaisons] OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, mars 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
[SAML2 Base]	OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, mars 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
[SAML2 Errata]	OASIS SAML V2.0 Approved Errata, 1 decembre 2009. http://www.oasis-open.org/committees/download.php/37166/sstc-saml-approved-errata-2.0-02.pdf
[SAML2 Méta]	OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, mars 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
[SAML2 MétaIU]	OASIS Working Draft 06, Metadata Extensions for Login and Discovery User Interface Version 1.0, novembre 2010 http://www.oasis-open.org/committees/download.php/40270/sstc-saml-metadata-ui-v1.0-wd06.pdf
[SAML2 Profils]	OASIS Standard, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, mars 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

2 Exigences (normatives) de la mise en place

2.1 Contraintes pour le Profil eGov 2.0 de l'initiative Kantara

Cette spécification s'articule autour de l'ensemble de spécifications SAML 2.0 [SAML2 *] et du profil SAML2 appelé « Kantara Initiative eGovernment Implementation Profile of SAML version 2.0 » [eGov 2.0].

Ce Profil de mise en place se fonde sur le Profil eGov 2.0 [eGov 2.0] publié par la Kantara Initiative, sans lui être parfaitement conforme, car cela n'est pas nécessaire (voir la note de la section 1.3, page 7). Bien que le Profil eGov 2.0 de Kantara soit un profil de « mise en œuvre » pour les fournisseurs de logiciels, le présent profil d'authentification électronique est un profil de « mise en place » qui restreint davantage et explique la mise en place des fournisseurs de services et des fournisseurs de services de justificatifs d'identité dans l'environnement d'authentification électronique du gouvernement du Canada. Dans les cas où le « *Profil de mise en place de l'ASI des STAE2* » n'offre pas explicitement d'orientation SAML2, la mise en œuvre doit se conformer aux exigences correspondantes SAML 2.0 d'OASIS.

Le tableau ci-dessous est établi selon l'ordre et la description des exigences des sections 2 et 3 du document [eGov 2.0], répétées telles quelles dans la première colonne. Le tableau indique le soutien requis de la part du Programme d'authentification électronique du gouvernement : en général, il s'agit d'un « prise en charge » ou d'une « contrainte » ou de l'indication « S.O. » (sans objet). Si d'autres détails s'avèrent nécessaires pour expliquer complètement l'exigence du gouvernement, ceux-ci sont présentés dans la troisième colonne.

En outre, des exigences supplémentaires, en plus des exigences eGov 2.0, sont précisées dans les sections qui suivent. L'authentification électronique impose également des contraintes aux spécifications SAML 2.0 et elle comporte peu d'exigences propres à l'authentification électronique.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
eGov 2.2 Metadata and Trust Management		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections. Additional expectations around the use of particular metadata elements related to profile behaviour may be encountered in those sections.	Prise en charge	
eGov 2.2.1 Metadata Profiles		
Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP].	Contrainte	Les mises en place de l'authentification électronique NE DOIVENT PAS utiliser la version 1.0 du Profil d'interopérabilité des métadonnées SAML V2.0 [MetaIOP].
In addition, implementations MUST support the use of the <md:KeyDescriptor> element as follows:	Prise en charge	
• Implementations MUST support the <ds:X509Certificate> element as input to subsequent requirements. Support for other key representations, and for other mechanisms for credential distribution, is OPTIONAL.	Contrainte	Aucun mécanisme FACULTATIF n'est pris en charge.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• Implementations MUST support some form of path validation of signing, TLS, and encryption credentials used to secure SAML exchanges against one or more trusted certificate authorities. Support for PKIX [RFC5280] is RECOMMENDED; implementations SHOULD document the behaviour of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].	Prise en charge	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.5, Sécurité.
• Implementations MUST support the use of OCSP [RFC2560] and Certificate Revocation Lists (CRLs) obtained via the "CRL Distribution Point" X.509 extension [RFC5280] for revocation checking of those credentials.	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.5, Sécurité.
• Implementations MAY support additional constraints on the contents of certificates used by particular entities, such as "subjectAltName" or "DN", key usage constraints, or policy extensions, but SHOULD document such features and make them optional to enable where possible.	Contrainte	Aucune contrainte supplémentaire FACULTATIVE n'est prise en charge.
Note that these metadata profiles are intended to be mutually exclusive within a given deployment context; they are alternatives, rather than complimentary or compatible uses of the same metadata information.	S.O.	

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension mechanism.	Prise en charge	
eGov 2.2.2 Metadata Exchange		
It is OPTIONAL for implementations to support the generation or exportation of metadata, but implementations MUST support the publication of metadata using the Well-Known-Location method defined in section 4.1 of [SAML2 Meta] (under the assumption that entityID values used are suitable for such support).	Contrainte	L'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) conserve et distribue les métadonnées à jour. Pour mettre un terme à l'utilisation de métadonnées non à jour par les membres de la fédération, l'OGFJGC interrompt la distribution de ces données. De plus, l'OGFJGC peut annuler un certificat dans le fichier de métadonnées, notamment en vue de mettre un terme à la participation d'un membre de la fédération ou encore en raison de la compromission d'un certificat et de changements de clé. • Les membres de la fédération DOIVENT présenter le document des métadonnées XML à l'OGFJGC. • Les membres de la fédération ne DOIVENT accepter que les documents de métadonnées XML qui proviennent de l'OGFJGC.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations MUST support the following mechanisms for the importation of metadata: • local file • remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL [RFC2818] In the case of HTTP resolution, implementations MUST support use of the "ETag" and "Last-Modified" headers for cache management. Implementations SHOULD support the use of more than one fixed location for the importation of metadata, but MAY leave their behaviour unspecified if a single entity's metadata is present in more than one source.	Contrainte	L'Organe de gouvernance de la fédération des justificatifs du GC assure l'actualisation et la distribution des métadonnées à jour, comme on le décrit ci-dessus. Toute procédure additionnelle sera établie par l'OGFJGC.
Importation of multiple entities' metadata contained within an <md:EntitiesDescriptor> element MUST be supported.	Contrainte	L'importation de métadonnées d'entités multiples contenues dans un élément <md:EntitiesDescriptor> DOIT être prise en charge. L'Organe de gouvernance de la fédération des justificatifs du GC assure l'actualisation et la distribution des métadonnées à jour. S'il y a lieu, il est possible de modifier le processus de distribution de manière à permettre les logiciels de fournisseurs qui ne prennent pas en charge l'importation de métadonnées d'entités multiples contenues dans un élément <md:EntitiesDescriptor>.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without service degradation or interruption.	Prise en charge	
eGov 2.2.2.1 Metadata Verification		
Verification of metadata, if supported, MUST include XML signature verification at least at the root element level, and SHOULD support the following mechanisms for signature key trust establishment: • Direct comparison against known keys. • Some form of path-based certificate validation against one or more trusted certificate authorities, along with certificate revocation lists and/or OCSP [RFC2560]. Support for PKIX [RFC5280] is RECOMMENDED; implementations SHOULD document the behaviour of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280].	Contrainte	• Les membres de la fédération DOIVENT signer leurs métadonnées à l'aide du certificat de signature remis par les services de gestion des justificatifs internes (GFI) du gouvernement. • Au moment de la consommation, le membre de la fédération qui fait appel aux métadonnées DOIT s'assurer que le certificat employé pour signer les métadonnées n'a pas été annulé. o Seules les Listes de certificats révoqués (LCR) sont prises en charge.
eGov 2.3 Name Identifiers		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]: • urn:oasis:names:tc:SAML:2.0:nameid-format:persistent • urn:oasis:names:tc:SAML:2.0:nameid-format:transient	Contrainte	Les mises en place de l'authentification électronique DOIVENT prendre en charge les éléments persistants. Les mises en place de l'authentification électronique ne DOIVENT pas prendre en charge les éléments transitoires.
Support for other formats is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge d'autres formats.
eGov 2.4 Attributes		
In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the generation and consumption of <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500].	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences de la section 2.4.1, Attributs d'assertion requis.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
The ability to support <saml2:AttributeValue> elements whose values are not simple strings (e.g., <saml2:NameID>, or other XML values) is OPTIONAL. Such content could be base64-encoded as an alternative.	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.1, Attributs d'assertion requis.
eGov 2.5 Browser Single Sign-On		
This section defines an implementation profile of the SAML V2.0 Web Browser SSO Profile [SAML2Prof].	Prise en charge	
eGov 2.5.1 Identity Provider Discovery		
Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery Service Protocol Profile in conformance with section 2.4.1 of [IDPDisco].	Contrainte	Les mises en place de l'authentification électronique DOIVENT prendre en charge le profil de dépistage du fournisseur de services de justificatifs d'identité précisé dans le document [SAML2 Profils]. Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge le profil du protocole de service de dépistage du fournisseur de services de justificatifs d'identité précisé dans le document [SAML2 Dépistage].
eGov 2.5.2 Authentication Requests		
eGov 2.5.2.1 Binding and Security Requirements		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of <saml2p:AuthnRequest> messages, including the generation or verification of signatures in conjunction with this binding.	Prise en charge	
Support for other bindings is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge d'autres liaisons.
eGov 2.5.2.2 Message Content		
In addition to standard core- and profile-driven requirements, Service Provider implementations MUST support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes (when appropriate):	Contrainte	Tel que précisé ci-dessous.
• AssertionConsumerServiceURL	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS utiliser l'adresse URL AssertionConsumerService. • Le fournisseur de services de justificatifs d'identité tire cette information des métadonnées.
• ProtocolBinding	Contrainte	S'il est présent, l'attribut ProtocolBinding DOIT être « urn:oasis:names:tc:SAML:2.0:bindings: HTTP-POST ».

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• ForceAuthn	Contrainte	On PEUT utiliser l'attribut ForceAuthn pour exiger que le fournisseur de services de justificatifs d'identité oblige l'utilisateur final à s'authentifier auprès du fournisseur, peu importe l'état de la session d'authentification de l'utilisateur dans le système du fournisseur de services de justificatifs d'identité. • Lorsqu'on utilise l'attribut ForceAuthn, le fournisseur de services de justificatifs d'identité ne doit pas changer son identificateur de nom par rapport à toute authentification précédente effectuée au cours de la session, même si cet identificateur est périmé. • Si on utilise l'attribut ForceAuthn et si l'authentification s'avère réussie, l'attribut AuthnInstant du fournisseur de services de justificatifs d'identité est réinitialisé pour l'utilisateur en question.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• IsPassive	Contrainte	• L'attribut IsPassive PEUT être utilisé si le fournisseur de services ne souhaite pas que le fournisseur de services de justificatifs d'identité commande directement le navigateur de l'utilisateur (par exemple, afficher une page à l'intention de l'utilisateur). • Si l'attribut IsPassive est vrai, l'utilisateur DOIT être en mesure de s'authentifier de manière passive, sinon la réponse produite ne DOIT PAS comprendre d'attribut <Assertion>. • Cette caractéristique permet au fournisseur de services de déterminer s'il doit aviser l'utilisateur qu'il ou elle est sur le point d'interagir avec le fournisseur de services de justificatifs d'identité. Voici un exemple de situation passive : le fournisseur de services s'aperçoit, à l'aide du témoin du domaine commun, que l'utilisateur peut avoir une session en cours dans le système d'un fournisseur de services de justificatifs d'identité particulier.
• AttributeConsumingServiceIndex	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS préciser l'attribut AttributeConsumingServiceIndex.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• <saml2p:RequestedAuthnContext>	Contrainte	• La demande d'authentification DOIT comprendre l'élément <RequestedAuthnContext>. • L'élément <RequestedAuthnContext> DOIT comprendre un niveau d'assurance, conformément aux précisions du document [SAML2 Assurance]. Les niveaux d'assurance de l'authentification électronique du gouvernement sont définis à la section 2.4.2 Niveaux d'assurance de l'authentification électronique du gouvernement. • Les fournisseurs de services DOIVENT demander un niveau d'assurance particulier à l'aide de l'opérateur de comparaison « exact ». • Le fournisseur de services PEUT demander plus d'un niveau d'assurance, par ordre de priorité. Cette particularité peut s'avérer utile si, par exemple, le niveau 2 est exigé mais si le fournisseur de services est disposé à accepter le niveau 3 dans les cas où le niveau 2 n'est pas possible.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
• <saml2p:NameIDPolicy>	Contrainte	• L'attribut <SPNameQualifier> PEUT être présent. o L'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) peut établir des groupes d'affiliations de fournisseurs de services de la FJGC qui utiliseront des identifiants anonymes mais persistants (IAP). Dans ces cas-là, les fournisseurs de services PEUVENT utiliser l'attribut <SPNameQualifier> dans la demande d'authentification pour indiquer leur souhait d'utiliser un IAP commun. • L'attribut <NameIDPolicy> peut contenir l'attribut AllowCreate. o En général, la valeur de l'attribut AllowCreate est « vrai », de sorte que si l'utilisateur n'a jamais fait appel au fournisseur de services de justificatifs d'identité sélectionné pour accéder au fournisseur de services, un identificateur puisse être créé à son intention et des messages SAML puisse être échangés entre les parties. o Toutefois, il peut être utile de donner la valeur « faux »à l'attribut AllowCreate si le fournisseur de services souhaite désactiver le traitement de l'inscription de justificatifs dans l'interface utilisateur du fournisseur de services de justificatifs d'identité. • Si l'attribut Format est présent il DOIT

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options. However, implementations MUST fully support the options enumerated above, and be configurable to utilize those options in a useful manner as defined by [SAML2Core].	Prise en charge	
Implementations MAY limit their support of the <saml2p:RequestedAuthnContext> element to the value "exact" for the Comparison attribute, but MUST otherwise support any allowable content of the element.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT prendre en charge que la valeur « exact » pour l'attribut Comparison.
Identity Provider implementations MUST support verification of requested AssertionConsumerServiceURL locations via comparison to <md:AssertionConsumerService> elements supplied via metadata using case-sensitive string comparison. It is OPTIONAL to support other means of comparison (e.g., canonicalization or other manipulation of URL values) or alternative verification mechanisms.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT prendre en charge aucune autre méthode de comparaison.
eGov 2.5.3 Responses		
eGov 2.5.3.1 Binding and Security Requirements		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST and HTTP-Artifact bindings [SAML2Bind] for the transmission of <saml2p:Response> messages.	Contrainte	Les mises en place de l'authentification électronique DOIVENT prendre en charge les liaisons HTTP POST. Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge les liaisons HTTP Artifact.
Support for other bindings, and for artifact types other than urn:oasis:names:tc:SAML:2.0:artifact-04, is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge d'autres liaisons.
Identity Provider and Service Provider implementations MUST support the generation and consumption of unsolicited <saml2p:Response> messages (i.e., responses that are not the result of a <saml2p:AuthnRequest> message).	Contrainte	Les mises en place de l'authentification électronique DOIVENT supprimer les messages <saml2p:Response> non sollicités. • Aucun cas d'utilisation de l'authentification électronique répertorié n'avait besoin de ces messages.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST support the issuance of <saml2p:Response> messages (with appropriate status codes) in the event of an error condition, provided that the user agent remains available and an acceptable location to which to deliver the response is available. The criteria for "acceptability" of a response location are not formally specified, but are subject to Identity Provider policy and reflect its responsibility to protect users from being sent to untrusted or possibly malicious parties. Note that this is a stronger requirement than the comparable language in [SAML2Prof].	Prise en charge	Pour l'OGFJGC, « l'acceptabilité d'un emplacement de réponse » indique que les métadonnées ont enregistré l'élément <AssertionConsumerServiceURL>.
Identity Provider and Service Provider implementations MUST support the signing of <saml2:Assertion> elements in responses; support for signing of the <saml2p:Response> element is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge la signature de l'élément <saml2p:Response>.
Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedAssertion> element when using the HTTP-POST binding; support for the <saml2:EncryptedID> and <saml2:EncryptedAttribute> elements is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS installer le soutien FACULTATIF.
eGov 2.5.3.2 Message Content		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of <saml2:Assertion>, <saml2:AuthnStatement>, and <saml2:AttributeStatement> elements in the <saml2p:Response> message to be limited to one. In turn, Service Provider implementations MAY limit support to a single instance of those elements when processing <saml2p:Response> messages.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT envoyer que les messages <saml2p:Response> qui contiennent au moins un élément <saml2:Assertion> unique.
Identity Provider implementations MUST support the inclusion of a Consent attribute in <saml2p:Response> messages, and a SessionIndex attribute in <saml2:AuthnStatement> elements.	Contrainte	Les mises en place de l'authentification électronique par des FSJ ne DOIVENT PAS inclure un attribut Consent dans les messages <saml2p:Response> Il n'existe actuellement aucun cas d'utilisation de l'authentification
Service Provider implementations that provide some form of session semantics MUST support the <saml2:AuthnStatement> element's SessionNotOnOrAfter attribute.	Prise en charge	Pour connaître les contraintes imposées aux mises en place de l'authentification électronique du fournisseur de services de justificatifs d'identité, reportez-vous à la section 2.2

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Service Provider implementations MUST support the acceptance/rejection of assertions based on the content of the <saml2:AuthnStatement> element's <saml2:AuthnContext> element. Implementations also MUST support the acceptance/rejection of particular <saml2:AuthnContext> content based on the identity of the Identity Provider. [IAP] provides one such mechanism via SAML V2.0 metadata and is RECOMMENDED; though this specification is in draft form, the technical details are not expected to change prior to eventual approval.	Prise en charge	
eGov 2.5.4 Artifact Resolution		
Pursuant to the requirement in section 2.5.3.1 for support of the HTTP-Artifact binding [SAML2Bind] for the transmission of <saml2p:Response> messages, implementations MUST support the SAML V2.0 Artifact Resolution profile [SAML2Prof] as constrained by the following subsections.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge la liaison HTTP-Artifact.
eGov 2.5.4.1 Artifact Resolution Requests		
Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResolve> messages.	S.O.	

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate requests; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	S.O.	
eGov 2.5.4.2 Artifact Resolution Responses		
Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResponse> messages.	S.O.	
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate responses; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	S.O.	
eGov 2.6 Browser Holder of Key Single Sign-On		
This section defines an implementation profile of the SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0 [HoKSSO].	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre cette fonction en charge.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
The implementation requirements defined in section 2.5 for the non-holder-of-key profile apply to implementations of this profile.	S.O.	
eGov 2.7 SAML 2.0 Proxying		
Section 3.4.1.5 of [SAML2Core] defines a formalized approach to proxying the SAML 2.0 Authentication Request protocol between multiple Identity Providers. This section defines an implementation profile for this behaviour suitable for composition with the Single Sign-On profiles defined in sections 2.5 and 2.6.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
The requirements of the profile are imposed on Identity Provider implementations acting as a proxy. These requirements are in addition to the technical requirements outlined in section 3.4.1.5.1 of [SAML2Core], which also MUST be supported.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
eGov 2.7.1 Authentication Requests		
Proxying Identity Provider implementations MUST support the mapping of incoming to outgoing <saml2p:RequestedAuthnContext> and <saml2p:NameIDPolicy> elements, such that deployers may choose to pass through values or map between different vocabularies as required.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Proxying Identity Provider implementations MUST support the suppression/eliding of <saml2p:RequesterID> elements from outgoing <saml2p:AuthnRequest> messages to allow for hiding the identity of the Service Provider from proxied Identity Providers.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
eGov 2.7.2 Responses		
Proxying Identity Provider implementations MUST support the mapping of incoming to outgoing <saml2:AuthnContext> elements, such that deployers may choose to pass through values or map between different vocabularies as required.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
Proxying Identity Provider implementations MUST support the suppression of <saml2:AuthenticatingAuthority> elements from outgoing <saml2:AuthnContext> elements to allow for hiding the identity of the proxied Identity Provider from Service Providers.	Prise en charge	Les mises en place de l'authentification électronique DOIVENT prendre en charge cet aspect lorsqu'elles sont configurées de manière à agir à titre de fournisseur de services de justificatifs d'identité de mise en cache.
eGov 2.8 Single Logout		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
This section defines an implementation profile of the SAML V2.0 Single Logout Profile [SAML2Prof]. For clarification, the technical requirements for each message type below reflect the intent to normatively require initiation of logout by a Service Provider using either the front- or back-channel, and initiation/propagation of logout by an Identity Provider using the back-channel.	Prise en charge	
eGov 2.8.1 Logout Requests		
eGov 2.8.1.1 Binding and Security Requirements		
Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the issuance of <saml2p:LogoutRequest> messages, and MUST support the SAML SOAP (using HTTP as a transport) and HTTP-Redirect bindings [SAML2Bind] for the reception of <saml2p:LogoutRequest> messages.	Prise en charge	
Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for both issuance and reception of <saml2p:LogoutRequest> messages.	Prise en charge	

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Support for other bindings is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique PEUVENT prendre en charge les liaisons http Redirect en vue de la production de messages <saml2p:LogoutRequest>. Aucune autre liaison n'est prise en charge.
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate <saml2p:LogoutRequest> messages; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	Contrainte	Les mises en place de l'authentification électronique DOIVENT respecter les exigences précisées à la section 2.4.5 Sécurité Sécurité
Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedID> element when using the HTTP-Redirect binding.	Prise en charge	
eGov 2.8.1.2 User Interface Behaviour		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST support both user-initiated termination of the local session only and user-initiated Single Logout. Upon receipt of a <saml2p:LogoutRequest> message via a front-channel binding, Identity Provider implementations MUST support user intervention governing the choice of propagating logout to other Service Providers, or limiting the operation to the Identity Provider. Of course, implementations MUST return status information to the requesting entity (e.g. partial logout indication) as appropriate.	Contrainte	Les mises en place de l'authentification électronique ne DOIVENT PAS prendre en charge les interventions de l'utilisateur qui régit la propagation de la fermeture de session à d'autres fournisseurs de services ou encore qui restreint le fonctionnement du fournisseur de services de justificatifs d'identité. • En tout temps, une demande de fermeture de session unique produit une fermeture de session globale pour la session principale.
Service Provider implementations MUST support both user-initiated termination of the local session only and user-initiated Single Logout.	Contrainte	Les mises en place de l'authentification électronique de fournisseur de services ne PEUVENT installer que le support de la fermeture de session unique (autrement dit la fermeture de session globale). • Les mises en place de l'authentification électronique de fournisseur de services de justificatifs d'identité DOIVENT propager la fermeture de session, sans intervention de la part de l'utilisateur, à tous les fournisseurs de services qui prennent part à la session et répondre au fournisseur de services initial.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Identity Provider implementations MUST also support the administrative initiation of Single Logout for any active session, subject to appropriate policy.	Prise en charge	L'OGFJGC indiquera s'il y a lieu, pour chaque mise en place de l'authentification électronique par des FSJ, quel soutien est nécessaire pour l'activation administrative de la fonction de fermeture de session unique.
eGov 2.8.2 Logout Responses		
eGov 2.8.2.1 Binding and Security Requirements		
Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) and HTTP-Redirect bindings [SAML2Bind] for the issuance of <saml2p:LogoutResponse> messages, and MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the reception of <saml2p:LogoutResponse> messages.	Contrainte	• Nota : Les liaisons HTTP Redirect utilisées pour l'envoi de messages <saml2p:LogoutResponse> sont à éviter et on ne doit les utiliser QUE SI le message <saml2p:LogoutRequest> a été envoyé à l'aide de cette liaison.
Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2 Bind] for both issuance and reception of <saml2p:LogoutResponse> messages.	Prise en charge	
Support for other bindings is OPTIONAL.	Contrainte	Les mises en place d'authentification électronique ne DOIVENT PAS installer de prise en charge FACULTATIVE.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate <saml2p:LogoutResponse> messages; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL.	Contrainte	Les mises en place d'authentification électronique ne DOIVENT PAS installer de prise en charge FACULTATIVE.
eGov 3 Conformance Classes		
eGov 3.1 Standard		
Conforming Identity Provider and/or Service Provider implementations MUST support the normative requirements in sections 2.2, 2.3, 2.4, and 2.5.	Prise en charge	
eGov 3.1.1 Signature and Encryption Algorithms		
Implementations MUST support the signature and digest algorithms identified by the following URIs in conjunction with the creation and verification of XML Signatures [XMLSig]: • http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (defined in [RFC4051]) • http://www.w3.org/2001/04/xmlenc#sha256 (defined in [XMLEnc])	Prise en charge	Cette exigence s'applique aux algorithmes utilisés pour la signature des messages SAML à codage URL, comme le décrit la section 3.4.4.1 du document [SAML-Liaisons].

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations SHOULD support the signature and digest algorithms identified by the following URIs in conjunction with the creation and verification of XML Signatures [XMLSig]: • http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 (defined in [RFC4051])	Prise en charge	
Implementations MUST support the block encryption algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]: • http://www.w3.org/2001/04/xmlenc#tripledes-cbc • http://www.w3.org/2001/04/xmlenc#aes128-cbc • http://www.w3.org/2001/04/xmlenc#aes256-cbc	Prise en charge	Il faut utiliser des algorithmes cryptographiques approuvés par le CSTC pour l'authentification électronique et les logiciels d'autorisation, comme le précise le document ISTA-11. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-fra.html (version actuelle).
Implementations MUST support the key transport algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]: • http://www.w3.org/2001/04/xmlenc#rsa-1_5 • http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	Contrainte	Il n'existe actuellement aucun cas d'utilisation au sein du GC qui nécessite cette exigence.

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Implementations SHOULD support the key agreement algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]: • http://www.w3.org/2009/xmlenc11#ECDH-ES defined in [XMLEnc11]) (This is a Last Call Working Draft of XML Encryption 1.1, and this normative requirement is contingent on W3C ratification of this specification without normative changes to this algorithm's definition.)	Prise en charge	Il faut utiliser des algorithmes cryptographiques approuvés par le CSTC pour l'authentification électronique et les logiciels d'autorisation, comme le précise le document ISTA-11. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-fra.html (version actuelle).
Support for other algorithms is OPTIONAL.	Contrainte	Les AE mises en place ne DOIVENT prendre en charge AUCUN autre algorithme.
eGov 3.2 Standard with Logout		
Conforming Identity Provider and/or Service Provider implementations MUST meet the conformance requirements in section 3.1, and MUST in addition support the normative requirements in section 2.8.	Contrainte	Voir la section 2.8 ci-dessus.
eGov 3.3 Full		

eGov 2.0 (citation du document d'origine de l'initiative Kantara)	ASI des STAE Soutien requis	Détails sur la mise en place de l'authentification électronique
Conforming Identity Provider and/or Service Provider implementations MUST meet the conformance requirements in section 3.1, and MUST in addition support the normative requirements in sections 2.6, 2.7, and 2.8.	Contrainte	• Il ne FAUT PAS configurer les authentifications électroniques mises en place d'après la section 2.6. • Les authentifications électroniques mises en place doivent plutôt être configurées en conformité avec la section 2.7 si elles doivent faire office de fournisseur de services de justificatifs d'identité de mise en cache.
End of table		

2.2 Autres contraintes visant les spécifications [SAML2*]

Outre les contraintes imposées par le présent Profil de mise en place quant au Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, le présent document de mise en place de l'authentification électronique stipule d'autres contraintes pour les spécifications SAML 2.0 sous-jacentes publiées par le Security Services Technical Committee (SSTC) d'OASIS.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 2.7.2, ligne 1061 <SessionNotOnOrAfter>	Contrainte	La mise en place, par le fournisseur de services de justificatifs d'identité, de l'authentification électronique ne DOIT pas préciser l'attribut SessionNotOnOrAfter. Ainsi, le fournisseur de services peut fixer la durée voulue de son propre contexte de sécurité. • Si un fournisseur de services de justificatifs d'identité de la FJGC ne peut pas indiquer qu'il ne faut pas transmettre cette valeur, il doit alors préciser la valeur élevée fixée par l'OGFJGC.
[SAML2 Base] Section 3.2.1, ligne 1489 <saml:Issuer>	Contrainte	Demande d'authentification d'un fournisseur de services <saml:Issuer> • DOIT être présent. • DOIT être le code d'entité entity_id attribué par l'OGFJGC. •

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 3.4.1, ligne 2017 <saml:Subject>	Contrainte	La demande d'authentification d'un fournisseur de services <saml:Subject> : ne DOIT PAS être incluse. • Aucun cas d'utilisation de l'authentification électronique n'exige l'élément <saml:Subject>.
[SAML2 Base] Section 3.4.1, ligne 2029 <saml:Conditions>	Contrainte	La demande d'authentification d'un fournisseur de services <saml:Conditions> : ne DOIT PAS être incluse. • Aucun cas d'utilisation de l'authentification électronique n'exige l'élément <saml:Conditions>.
[SAML2 Base] Section 3.4.1, ligne 2068 ProtocolBinding	Contrainte	La demande d'authentification d'un fournisseur de services ProtocolBinding • PEUT être utilisée. • Si l'attribut ProtocolBinding est présent, il doit préciser : « urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST ».

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 3.6.1, ligne 2421 <ManageNameIDRequest>	Contrainte	Les mises en place des fournisseurs de services de justificatifs d'identité DOIVENT transmettre en temps opportun un élément <ManageNameIDRequest> avec <Terminate> dans le cas d'un justificatif qui a été révoqué, à tout fournisseur de services qui dispose d'un point de terminaison défini pour l'élément <ManageNameIDService> et pour lequel il a déjà envoyé une assertion pour l'utilisateur. Les mises en place des fournisseurs de services de justificatifs d'identité ne DOIVENT envoyer aucun autre message <ManageNameIDRequest>. Les mises en place des fournisseurs de services DOIVENT répondre aux messages <ManageNameIDRequest>.
		•
[SAML2 Liaisons] Section 3.5.3, ligne 785 <RelayState>	Contrainte	L'attribut <RelayState> ne PEUT PAS être adjoint à un message de réponse, sauf s'il a été fourni dans le message de demande correspondant.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Assurance] Section 3, ligne 276 <assurance-certification>	Contrainte	Les métadonnées des fournisseurs de services de justificatifs d'identité de l'authentification électronique DOIVENT préciser le ou les niveaux d'assurance pris en charge par l'attribut <assurance-certification>, selon la définition qui figure à la section 3, Identity Assurance Certification Attribute Profile (profil des attributs de certification de l'assurance de l'identité), du document [SAML2 Assurance]. La section 2.4.2, Niveaux d'assurance de l'authentification électronique du gouvernement, précisent les valeurs URI à utiliser pour les quatre niveaux d'assurance. Plusieurs valeurs de niveau d'assurance PEUVENT être précisées dans les métadonnées des fournisseurs de services d'identité, mais une seule valeur est renvoyée dans une réponse d'authentification.
[SAML2 Méta] Section 2.3.2, ligne 371 <entityID>	Contrainte	L'entité et l'OGFJGC DOIVENT convenir de l'attribut <entityID>.
[SAML2 Meta] Section 2.3.2.1, ligne 443 <Organization>	Contrainte	Il est PRÉFÉRABLE d'inclure l'attribut <Organization> et d'indiquer OrganizationName ou OrganizationDisplayName.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Méta] Section 2.3.2.2, ligne 476 <ContactPerson>	Contrainte	Il est PRÉFÉRABLE d'inclure l'attribut <ContactPerson>. L'authentification électronique propose d'ajouter l'adresse de courriel (EmailAddress) ou le numéro de téléphone (TelephoneNumber).
[SAML2 Méta] Section 2.4.1, ligne 550 <RoleDescriptor>	Contrainte	• L'élément de métadonnées <RoleDescriptor> ne DOIT PAS être utilisé.
[SAML2 Méta] Section 2.4.3, ligne 683 <IDPSSODescriptor> y compris la Section 2.4.2, ligne 643 <SSODescriptorType>	Contrainte	• L'attribut WantAuthnRequestsSigned DOIT indiquer la valeur « true ». • Deux attributs <SingleLogoutService> DOIVENT être présents (un pour chacune des liaisons : SOAP et HTTP Redirect). • Un seul attribut <SingleSignOnService> DOIT être présent. • Un seul attribut < ManageNameIDService> DOIT être présent en vue de la réception des réponses aux messages de terminaison NameID. La liaison précisée DOIT être : urn:oasis:names:tc:SAML:2.0:bindings:SOAP.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Méta] Section 2.4.4, ligne 736 <SPSSODescriptor> y compris la Section 2.4.2, ligne 643 <SSODescriptorType>	Contrainte	• L'attribut AuthnRequestsSigned DOIT indiquer la valeur « true ». • L'attribut WantAssertionsSigned DOIT indiquer la valeur « true ». • L'attribut <AssertionConsumerService> DOIT être inclus. • Un seul attribut <AssertionConsumerService> DOIT disposer de la liaison urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST. • Un seul attribut < ManageNameIDService> PEUT être présent pour indiquer l'envoi des messages de terminaison NameID par les fournisseurs de services d'identité. La liaison DOIT être : urn:oasis:names:tc:SAML:2.0:bindings:SOAP.
[SAML2 Méta] Section 2.4.5, ligne 828 <AuthnAuthorityDescriptor>	Contrainte	L'attribut <AuthnAuthorityDescriptor> ne DOIT PAS être utilisé.
[SAML2 Méta] Section 2.4.6, ligne 861 <PDPDescriptor>	Contrainte	L'attribut <PDPDescriptor> ne DOIT PAS être utilisé.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
[SAML2 Méta] Section 2.5, ligne 938 <AffiliationDescriptor>	Contrainte	L'attribut <AffiliationDescriptor> PEUT être utilisé. • L'Organe de gouvernance de la fédération des justificatifs du GC (OGFJGC) peut établir des groupes d'affiliations de fournisseurs de services de la FJGC qui utiliseront des identifiants anonymes mais persistants (IAP). Dans ces cas-là. L'OGFJGC fournira des métadonnées définissant ces groupes.
[SAML2 MétaIU] Section 2.1.1 <md:UIInfo>	Prise en charge	Les métadonnées du fournisseur de services PEUVENT comprendre les éléments <mdui:DisplayName> et <mdui:Logo>. Le fournisseur de services de justificatifs d'identité PEUT utiliser ces éléments de métadonnées pour informer l'utilisateur au sujet de l'entité qui demande une authentification pendant le dialogue d'authentification associé.
Fin du tableau		

2.3 Autres extensions liées à la spécification [SAML2 *]

Outre les contraintes imposées par ce Profil de mise en place quant au Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, le présent document de mise en place de l'authentification électronique élargit également les spécifications SAML 2.0 sous-jacentes publiées par le Security Services Technical Committee (SSTC) d'OASIS.

SAML2 *	ASI STAE Soutien requis	Détails de la mise en place de l'authentification électronique
Aucune exigence définie		
Fin du tableau		

2.4 Autres exigences du gouvernement

Outre les contraintes imposées par ce Profil de mise en place au Profil eGov 2.0 [eGov 2.0] publié par l'initiative Kantara, et les autres contraintes et extensions appliquées aux spécifications SAML 2.0 publiées par le Security Services Technical Committee (SSTC) d'OASIS, le présent document de mise en place de l'authentification électronique impose également d'autres exigences à l'environnement d'authentification électronique du gouvernement.

2.4.1 Attributs d'assertion requis

Exigence quant à l'authentification électronique	ASI STAE Prise en charge requise	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 2.7.3, ligne 1165 <AttributeStatement>	Extension	Les mises en place de l'authentification électronique par les fournisseurs de services et les fournisseurs de services de justificatifs d'identité DOIVENT prendre en charge les attributs obligatoires de l'authentification électronique : • Ceux-ci sont indiqués à la section 2.4.1.1 Attributs obligatoires

Exigence quant à l'authentification électronique	ASI STAE Prise en charge requise	Détails de la mise en place de l'authentification électronique
[SAML2 Base] Section 2.7.3, ligne 1165 <AttributeStatement>	Extension	Les mises en place de l'authentification électronique par les fournisseurs de services de justificatifs d'identité PEUVENT prendre en charge des attributs facultatifs de l'authentification électronique : • Ceux-ci sont indiqués à la section 2.4.1.2 Attributs facultatifs
[SAML2 Base] Section 2.7.3, ligne 1165 <AttributeStatement>	Contrainte	Les mises en place de l'authentification électronique par les fournisseurs de services ne DOIVENT PAS prendre en charge la réception d'autres attributs. • Les mises en place de l'authentification électronique par les fournisseurs de services DOIVENT rejeter tout autre attribut et elles ne doivent pas utiliser les valeurs de ces attributs dans le traitement.
Fin du tableau		

2.4.1.1 Attributs obligatoires

Nom (URI)	Description	Format	Type de données
ca:gc:cyber-authentication:basic:specVer	Version de la spécification de l'interface	DOIT être « 2.0 » pour cette spécification d'interface [ASI STAE 2]	xs:chaîne

Nom (URI)	Description	Format	Type de données
Fin du tableau			

2.4.1.2 Attributs facultatifs

Nom (URI)	Description	Format	Type de données
ca:gc:cyber-authentication:basic:assuranceLevel	À éviter : n'est inclus que pour la transition depuis la version 1 de l'[ASI STAE 1] Degré de confiance du mécanisme d'authentification final.	DOIT être : 1, 2, 3, 4 ou test	xs:chaîne
urn:oid: 2.16.840.1.113730.3.1.39	À éviter : n'est inclus que pour la transition depuis la version 1 de l'[ASI STAE 1] Langue préférée de l'utilisateur final (celle-ci doit normalement être définie lorsque l'utilisateur change de langue pendant l'interaction avec le fournisseur de services de justificatifs d'identité).	DOIT être conforme à la définition du champ de l'en-tête Accept-Language défini, une exception prévalant cependant : la séquence "Accept-Language" ":" doit être omise.	xs:chaîne
Fin du tableau			

2.4.2 Niveaux d'assurance de l'authentification électronique du gouvernement

Les demandes et les réponses d'authentification sur les justificatifs de l'authentification électronique du gouvernement feront preuve du niveau d'assurance du gouvernement du Canada requis. Au total, quatre niveaux d'assurance sont définis dans [ITSG-31] et utilisés par le programme d'authentification électronique du gouvernement. Les valeurs des URI qui représentent ces niveaux d'assurance du gouvernement du Canada sont les suivantes :

- http://cyber-auth.gc.ca/assurance/loa1
- http://cyber-auth.gc.ca/assurance/loa2
- http://cyber-auth.gc.ca/assurance/loa3
- http://cyber-auth.gc.ca/assurance/loa4

Les schémas qui correspondent à ces valeurs sont offerts par l'OGFJ du gouvernement.

2.4.3 Communication des préférences linguistiques

Afin de respecter les exigences de la politique du gouvernement, il fallait disposer d'une méthode d'envoi de la langue préférée actuellement par l'utilisateur (et non celle du navigateur) du fournisseur de services au fournisseur de services de justificatifs d'identité et du fournisseur de services de justificatifs d'identité au fournisseur de services dans tous les cas, même dans les cas où l'authentification échoue et aucune assertion n'est produite. À cet égard, l'authentification électronique fait appel à un témoin de session qui figure dans un domaine commun défini par l'OGFJGC (il peut s'agir du même domaine que celui établi pour le profil de dépistage du fournisseur de services de justificatifs d'identité).

Ce témoin de session comprend l'attribut de langue, dont les valeurs sont définies dans le document [RFC 1766]. Les valeurs admises pour l'attribut de langue de l'authentification électronique sont indiquées ci-dessous:

- en (anglais)
- fr (français)

Les fournisseurs de services et les fournisseurs de services de justificatifs d'identité DOIVENT lire ce témoin et utiliser le paramètre de langue pour les pages d'interface utilisateur qui sont affichées.

Les fournisseurs de services et les fournisseurs de services de justificatifs d'identité DOIVENT veiller à ce que ce témoin précise la langue préférée de l'utilisateur avant de transmettre un message sur une liaison HTTP-Redirect ou HTTP-Post. Étant donné que ce

témoin de langue du gouvernement sera sans doute utilisé, que l'utilisateur se trouve ou non dans une situation de demande/réponse d'authentification, il doit être mis à jour dans les plus brefs délais.

Une annexe du présent document décrit les détails du témoin de langue du gouvernement dans le domaine commun.

2.4.4 Protocole de gestion d'identificateur de nom

Différents ministères du gouvernement exigent un avis en cas d'annulation de justificatif. Pour prendre cette fonction en charge, le document [ASI des STAE2] ajoute le soutien du protocole (et du profil) de gestion d'identificateur de nom SAML.

Les fournisseurs de services précisent s'ils souhaitent recevoir ces messages en adjoignant un élément <ManageNameIDService> à leur SPSSODescriptor dans les métadonnées du fournisseur de services.

Les FSJ DOIVENT envoyer une demande <ManageNameIDRequest> aux fournisseurs de services lorsqu'ils révoquent un code d'utilisateur utilisé auparavant par ces derniers. Les FSJ DOIVENT informer un fournisseur de services de l'annulation d'un code d'utilisateur (NameID) s'ils ont déjà transmis à ce fournisseur de services des assertions pour l'utilisateur visé, et ne DOIVENT PAS envoyer un tel avis d'annulation de code d'utilisateur NameID à d'autres fournisseurs de services. Les avis d'annulation doivent être transmis en temps opportun via le canal d'appui, selon une méthode approuvée par l'OGFJGC. À cette fin, les FSJ DOIVENT ajouter un élément <ManageNameIDService> à leur descripteur IDPSSODescriptor dans leurs métadonnées. La STAE2 utilise des identificateurs anonymes mais persistants (IAP), c'est-à-dire des identificateurs persistants SAML [SAML2 BASE, 3.7] et [SAML2 Errata, E78].. Pour cette raison, les FSJ doivent attribuer « …un identificateur opaque persistant à chaque utilisateur... ». Par ailleurs, « une valeur donnée, une fois associé à un utilisateur, NE DOIT JAMAIS être attribué à un autre utilisateur ».

2.4.5 Sécurité

Pour établir des communications fiables et sûres, cette spécification d'interface est largement tributaire des paires de clés cryptographiques X.509v3. La présente section décrit les différents certificats nécessaires ainsi que les détails de l'utilisation de ceux-ci.

2.4.5.1 Certificats des Services de gestion des justificatifs internes (GFI) du gouvernement

Les Services de gestion des justificatifs internes (GFI) du gouvernement, qui sont exploités par TPSGC pour le compte du gouvernement, assurent la fiabilité et la sécurité de la fédération des justificatifs du gouvernement. Toute interopération au sein de la fédération des justificatifs du GC nécessite la possession de certificats valides émis par les services de GFI. Les services de GFI remettent trois certificats à chaque fournisseur de services (un est utilisé pour TLS, un pour la signature numérique et un troisième

pour le chiffrement) et deux certificats à chaque fournisseur de services de justificatifs d'identité (un pour TLS et un autre pour la signature numérique).

- Ces certificats DOIVENT être conservés en conformité avec les responsabilités de l'abonné (que précise l'OGFJGC).

2.4.5.2 Signature numérique

Les expéditeurs de tous les messages SAML, et des parties de ceux-ci, DOIVENT signer ces messages à l'aide du certificat de signature des services de GFI du gouvernement qui leur a été remis. À l'aide de la signature, le destinataire du message peut authentifier l'expéditeur et confirmer que le message n'a pas été modifié depuis l'apposition de la signature.

- Une fois qu'il a reçu le message, le destinataire DOIT authentifier l'expéditeur et vérifier la signature.
- Le destinataire DOIT vérifier si le certificat de l'expéditeur qui a servi à signer le message a été annulé. Pour effectuer cette vérification, les systèmes membres de la fédération DOIVENT utiliser la méthode ci-dessous :
    - Liste de certificats révoqués (LCR) – L'emplacement de la LCR (dans le répertoire ou au site Web) peut être configuré de manière fixe dans le logiciel; la LCR est par la suite téléchargée périodiquement. Pour obtenir plus de détails sur l'emplacement des noms distinctifs et le nom d'hôte du répertoire, veuillez consulter la documentation sur le GFI du GC de l'OGFJGC.
- Si l'état du certificat (annulé ou non) ne peut pas être déterminé, le système membre de la fédération DOIT rejeter le message correspondant.

2.4.5.3 Chiffrement

Le chiffrement permet de s'assurer que seul le destinataire prévu est en mesure de déchiffre le message et lire l'information confidentielle qu'il renferme.

- Toute l'information confidentielle d'un message SAML DOIT être chiffrée.
- Le chiffrement DOIT utiliser la clé publique du certificat de chiffrement remis par les services de GFI du gouvernement au destinataire prévu.

2.4.5.4 Sites Web de TLS

2.4.5.4.1 Pour les liaisons de canal d'avant-plan

Cette spécification d'interface précise les liaisons de canal d'avant plan qui utilisent http sur TLS (HTTPS) pour la transmission des messages.

- Les sites gérés par les membres de la fédération qui utilisent les liaisons HTTP sur TLS DOIVENT doivent protéger les sessions TLS à l'aide d'un certificat accepté par défaut par les navigateurs commerciaux.
- L'utilisation de SSLv3.0/TLS doit être conforme aux lignes directrices du CST (par exemple ASTI-11G) et aux politiques ministérielles.
- La liaison HTTPS sur TLS (v1.1 ou supérieure) DOIT être utilisée, sauf si elle n'est pas prise en charge par le navigateur.
- La liaison HTTPS sur TLS (v1.0) PEUT être utilisée.
- La liaison HTTPS sur SSL (v3.0 ou supérieure) ne PEUT être utilisée que si le protocole TLS (v1.0 ou supérieure) n'est pas pris en charge par le navigateur.
- Les versions antérieures du protocole SSL ne DOIVENT PAS être utilisées.

2.4.5.4.2 Pour les liaisons de canal d'appui

Cette spécification d'interface précise les liaisons de canal d'appui qui utilisent SOAP sur TLS pour le transport des messages.

- Les sites gérés par les membres de la fédération qui utilisent les liaisons SOAP sur TLS DOIVENT doivent protéger les sessions TLS à l'aide d'un certificat remis par les services de GFI du gouvernement.
- L'utilisation de SSLv3.0/TLS doit être conforme aux lignes directrices du CST (par exemple ASTI-11G) et aux politiques ministérielles.
- Le protocole TLS (v1.1 ou supérieure) DOIT être utilisé.
- Les versions antérieures du protocole TLS ou SSL ne DOIVENT PAS être utilisées.

2.4.6 Traitement des exceptions

Prise en charge de l'interface d'authentification électronique requise	Détails de la mise en place de l'authentification électronique
Le service SAML d'un membre de l'authentification électronique DOIT traiter les erreurs sans accroc.	Plus particulièrement, le service SAML d'un membre de l'authentification électronique DOIT traiter la liste des erreurs possibles indiquées à la section 2.4.6.1, Erreurs à traiter .

2.4.6.1 Erreurs à traiter

Le tableau ci-après présente les erreurs que le service SAML d'un membre de l'authentification électronique DOIT traiter sans accroc (autrement dit d'une façon conviviale et contrôlée, conformément à la capacité du fournisseur de services de justificatifs d'identité ou du fournisseur de services de répondre). Le tableau catégorise les erreurs d'après les événements SAML.

Erreur
Erreur dans le traitement de la <Response> (réponse) • <Issuer> (expéditeur) incorrect ou inconnu • Version incorrecte • Incorrect Version • InResponseTo (en réponse à) non reconnu • IssueInstant (envoi) inacceptable • L'état indiqué n'est pas la réussite

Erreur dans le traitement de l'<Assertion> • Signature non valide • Certificat de signature révoqué • Impossible de déterminer l'état quant à la révocation • La durée de l'<Assertion> n'est pas valide • Impossible de déchiffrer l'<Assertion> • Destinataire incorrect • Version incorrecte
Erreur dans le traitement de <AuthnRequest> (demande d'authentification) • <Issuer> (expéditeur) inconnu • Signature non valide • Certificat de signature révoqué • Impossible de déterminer l'état quant à la révocation
Erreur dans le traitement de la demande de fermeture de session unique • <Issuer> (expéditeur) inconnu • Signature non valide • Certificat de signature révoqué • Impossible de déterminer l'état quant à la révocation

Erreur dans le traitement de la <Response> (réponse) SLO • <Issuer> (expéditeur) inconnu • Signature non valide • Certificat de signature révoqué • Impossible de déterminer l'état quant à la révocation

Annexe A: Autres fonctions en plus de l'authentification électronique (normatives)

A.1. Témoin de langue du GC

On présente ci-après une méthode à l'aide de laquelle le fournisseur de services ou le fournisseur de services de justificatifs d'identité peut déterminer la langue dont se sert actuellement l'utilisateur. Cette méthode fait appel à un témoin qui est stocké dans un domaine commun aux fournisseurs de services de justificatifs d'identité et aux fournisseurs de services dans la mise en place de la FJGC. Ce domaine est établi par l'OGFJGC et il peut être le même que le domaine commun utilisé pour le profil de dépistage du fournisseur de services de justificatifs d'identité; dans ce profil il s'appelle <common-domain> et le témoin qui renferme la dernière langue utilisée est le témoin de langue du GC.

Dans la FJGC, le fournisseur de services et le fournisseur de services de justificatifs d'identité doivent héberger des serveurs Web dans le domaine commun, comme l'indique l'OGFJGC.

A.1.1 Témoin de langue du GC stocké dans un domaine commun du GC

Le nom du témoin DOIT être « _gc_lang ». Le format de la valeur du témoin DOIT être celui d'une chaîne de texte monovaluée.

Le service de stockage de témoin dans le domaine commun (voir ci-après) DOIT mettre à jour le paramètre de langue si l'utilisateur indique une autre langue. Il s'agit ainsi que la dernière langée précisée figure dans le témoin. Les valeurs du témoin de langue du GC sont définies dans le document [RFC 1766]. Les valeurs acceptables pour le témoin de langue du GC sont les suivantes :

- en (anglais)
- fr (français)

Le témoin défini DOIT comporter le préfixe de chemin « / ». Le domaine précisé DOIT être « .<common-gc-domain> », <commun-gc-domaine> étant le domaine commun du GC établi par l'OGFJGC pour cette méthode (on peut également l'utiliser avec le profil de dépistage du fournisseur de services de justificatifs d'identité). Un point doit figurer au début. Le témoin DOIT être désigné comme étant sûr.

La syntaxe du témoin doit être conforme au document RFC 2965 de l'IETF. Le témoin ne DOIT concerner que la session en cours.

A.1.2 Obtention du témoin de langue du GC

Avant de présenter un dialogue d'authentification à l'utilisateur, le fournisseur de services de justificatifs d'identité DOIT connaître la langue choisir par cet utilisateur pour les communications. À cet égard, le fournisseur de services de justificatifs d'identité DOIT lancer un échange destiné à présenter le témoin de langue du GC au fournisseur de services de justificatifs d'identité après qu'il ait été lu par un serveur HTTP du domaine commun.

La méthode à l'aide de laquelle le fournisseur de services lit le témoin est propre à la mise en œuvre, pourvu que celle-ci soit en mesure d'amener l'agent de l'utilisateur à présenter des témoins qui ont été définis d'après les paramètres appropriés. Une stratégie de mise en œuvre acceptable est décrite ci-dessous; il ne s'agit pas d'une stratégie normalisée. De plus, elle peut ne pas être optimale pour certaines applications.

- Le fournisseur établit au préalable un pseudonyme DNS et IP à son intention dans le domaine commun.
- Renvoyer l'agent de l'utilisateur à lui-même à l'aide du pseudonyme DNS, à l'aide d'une URL qui précise « http » à titre de schéma URL. La structure de l'URL est propre à la mise en œuvre et elle peut comprendre l'information sur la session qui sert à identifier l'agent de l'utilisateur.
- Renvoyer l'agent de l'utilisateur, cette fois à lui-même.

A.1.3 Définition du témoin de langue du GC

Avant d'appeler une demande d'authentification, le fournisseur de services DOIT s'assurer que le témoin de langue du GC précise la langue choisir par l'utilisateur. Avant d'envoyer une réponse d'authentification électronique (y compris les réponses d'erreur), le fournisseur de services de justificatifs d'identité DOIT veiller à ce que le témoin de langue du GC soit défini en fonction de la langue choisie par l'utilisateur. Le fournisseur de services ou le fournisseur de services de justificatifs d'identité PEUT redéfinir le témoin de langue du GC si l'utilisateur change la langue. La méthode par laquelle le fournisseur de services le fournisseur de services ou le fournisseur de services de justificatifs d'identité définit le témoin est propre à la mise en œuvre, pourvu que le témoin soit défini correctement selon les paramètres indiqués ci-dessus. Une stratégie de mise en œuvre acceptable est présentée ci-dessous. Il ne s'agit pas d'une stratégie normalisée. Le fournisseur de services ou le fournisseur de services de justificatifs d'identité peut :

- Établir au préalable un pseudonyme DNS et IP à son intention dans le domaine commun.
- Renvoyer l'agent de l'utilisateur à lui-même à l'aide du pseudonyme DNS, à l'aide d'une URL qui précise « http » à titre de schéma URL. La structure de l'URL est propre à la mise en œuvre et elle peut comprendre l'information sur la session qui sert à identifier l'agent de l'utilisateur.
- Définir le témoin de l'agent de l'utilisateur renvoyé à l'aide des paramètres précisés ci-dessus.
- Renvoyer l'agent de l'utilisateur, cette fois à lui-même.