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
THERE IS A SECURITY REQUIREMENT ASSOCIATED WITH THIS SOLICITATION

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 ISS Transformation - RFP	
Solicitation No. - N° de l'invitation EP243-170549/B	**Amendment No. - N° modif.** 003
Client Reference No. - N° de référence du client 20170549	**Date** 2017-06-02
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 2017-07-14**	**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

Numéro de la modification : 003

Objectif :

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

A. MODIFICATIONS

Changement 21 :

À la PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT, **SUPPRIMER** les articles 7.4.2 à 7.4.7

RENUMÉROTER les articles 7.4.8, 7.4.9, 7.4.10 et 7.4.11 à 7.4.10, 7.4.11, 7.4.12 et 7.4.13, respectivement.

INSÉRER les articles 7.4.2 à 7.4.9, comme suit :

7.4.2 Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent être résidents permanents du Canada ou citoyens du Canada et doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ ou SECRET, comme requis, délivrées ou approuvée par la DSIC de TPSGC.

7.4.3 Les membres du personnel de l'entreprise qui doivent avoir accès aux biens ou aux renseignements OTAN NON-CLASSIFIÉS n'ont pas besoin d'avoir une attestation de sécurité ; toutefois, l'entrepreneur doit s'assurer que de tiers n'auront pas accès aux renseignements OTAN NON-CLASSIFIÉS et que le principe du « besoin de savoir », sera appliqué.

7.4.4 Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens NATO DIFFUSION RESTREINTE, doivent être résidents permanents du Canada ou citoyens du Canada et doivent TOUS détenir une cote de FIABILITÉ ou SECRET, comme requis, en vigueur, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

7.4.5 L'entrepreneur ou l'offrant NE DOIT PAS emporter de renseignements PROTÉGÉS hors des établissements de travail visés; et l'entrepreneur ou l'offrant doit s'assurer que son personnel est au courant de cette restriction et qu'il l'a respecté.

7.4.6 Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent pas être attribués sans l'autorisation écrite préalable de la DSIC de TPSGC.

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. Services publics et Approvisionnement Canada (SPAC) 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, SPAC 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 ».

7.4.8 En permanence pendant l'exécution du contrat, l'entrepreneur devrait détenir une lettre de SPAC indiquant les résultats de l'évaluation de la PCIE ainsi que le statut attribué à son en-treprise, c'est-à-dire « Sans PCIE » ou « Sans PCIE par atténuation ».

7.4.9 Tout changement au questionnaire et aux facteurs connexes d'évaluation de la PCIE doit être immédiatement signalé au Secteur de la sécurité industrielle aux fins de détermination de l'incidence du changement sur le statut lié à la PCIE.

Changement 22 :

À la PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

SUPPRIMER entièrement l'article 7.28 et le **REMPLACER** par le libellé suivant :

7.28 Services de transition à la fin du contrat

Douze mois avant l'expiration du contrat, l'entrepreneur doit préparer et fournir à l'autorité technique un plan détaillé de transition de sortie relatif aux services. À la suite de l'acceptation par l'autorité technique, l'entrepreneur doit transférer ses services à un autre fournisseur, conformément au plan, au cours de la période menant à la fin du contrat et jusqu'à trois mois par la suite. L'entrepreneur convient qu'il n'y aura aucuns frais pour ces services.

Changement 23 :

À l'ANNEXE A, partie 2, sous 2.2.1 Application de traitement du service :

SUPPRIMER :

APP-IM.16	Permettre et soutenir l'archivage des dossiers.

INSÉRER :

APP-IM.16	Permettre et soutenir l'archivage des dossiers au sein de la solution.

Changement 24 :

À l'ANNEXE A, partie 2, sous 2.2.1 Application de traitement du service :

SUPPRIMER :

APP-IM.27	Permettre aux utilisateurs internes de récupérer les enregistrements archivés d'un dossier de cas pendant une période donnée.

INSÉRER :

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.

Changement 25 :

À l'ANNEXE A, partie 2, sous 2.2.1 Application de traitement du service :

SUPPRIMER :

APP-COM.03	Permettre aux utilisateurs externes de recevoir automatiquement des notifications textuelles normalisées résultant d'événements préétablis comme des décisions prises au sujet de la demande de services.

INSÉRER :

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.

Changement 26 :

À l'ANNEXE A, partie 2, sous 2.2.1 Application de traitement du service :

SUPPRIMER :

AP-PPL.02	Permet de numériser les documents papier afin de les annexer aux dossiers de cas.

INSÉRER :

AP-PPL.02	Permet de joindre les documents numérisés aux dossiers de cas.

Changement 27 :

À l'ANNEXE A, partie 2, sous 2.2.2 Portail de services Web

SUPPRIMER :

WP-UE.09	Permet aux utilisateurs externes de recevoir des messages SMS normalisés au sujet de mises à jour sur les demandes de services.

INSÉRER :

WP-UE.09	Permet aux utilisateurs externes de recevoir des messages courriel normalisés au sujet de mises à jour sur les demandes de services.

Changement 28 :

À l'ANNEXE A, partie 2, sous 2.2.2 Portail de services Web

SUPPRIMER :

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.

Changement 29 :

À l'ANNEXE A, partie 3, sous 1.1 Exigence Aperçu

SUPPRIMER :

L'entrepreneur doit concevoir, développer, configurer, tester, mettre en oeuvre, déployer et stabiliser la solution, comme l'illustre la figure ci-dessous. La solution doit permettre les modifications, les rajustements ou les ajouts de flux de travaux de processus opérationnel, de fonctions automatisées de système, et d'autres processus et règles connexes, avec une modification minimale du code de l'application. La solution doit être conviviale, fiable, facile à entretenir, évolutive, interopérable et conforme aux politiques et lignes

directrices de GI/TI du GC et à son environnement.

INSÉRER :

L'entrepreneur doit concevoir, développer, configurer, tester, mettre en œuvre, déployer et stabiliser la solution, en utilisent comme recommandation, les technologies proposés par TPSGC indiquer si dessous. La solution doit permettre les modifications, les rajustements ou les ajouts de flux de travaux de processus opérationnel, de fonctions automatisées de système, et d'autres processus et règles connexes, avec une modification minimale du code de l'application. La solution doit être conviviale, fiable, facile à entretenir, évolutive, interopérable et conforme aux politiques et lignes directrices de GI/TI du GC et à son environnement.

Changement 30 :

SUPPRIMER :

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

Changement 31 :

À la partie 3, 1.1 Exigence Aperçu, paragraphe 3 :

SUPPRIMER :

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 du portail Web, fondé sur la technologie Adxstudio.

INSÉRER :

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 du portail Web.

Changement 32 :

À la partie 3, 1.1 Exigence Aperçu:

SUPPRIMER :

Cette architecture repose sur les suites Enterprise IT Target, utilisées par les directions des dirigeants principaux de l'information du SCT et de TPSGC, dans le but de rationaliser et normaliser l'empreinte de toutes les applications du GC. Dans la mesure du possible, l'entrepreneur doit respecter les exigences de la présente demande, y compris toute nouvelle exigence découlant de la réorganisation des processus opérationnels, en recourant aux technologies approuvées pour l'architecture d'entreprise du GC et de TPSGC, disponibles au sein de la chaîne d'approvisionnement des TI du GC ou de TPSGC. Si ce n'est pas possible, les technologies de rechange proposées devront être approuvées par le GC et un plan pour la migration de ces technologies de rechange au sein de l'empreinte technologique du GC ou de TPSGC devra être élaboré et fourni avec la proposition de solution. Tous les éléments de la solution qui relèvent de la portée du présent projet doivent intégrer les éléments de TI utilisés par le GC et respecter l'exigence d'une solution unifiée. L'accès contrôlé pour les utilisateurs externes se fera par l'intermédiaire d'une interface de portail Web centrée sur l'utilisateur.

Les suites mentionnées auxquelles l'entrepreneur doit se conformer comprennent, entre autres, les suivantes :

(a) **Adxstudio Portals** (portails Adxstudio ou formulaires Web ASP.NET)
Technologie de portail – Le portail doit être développé à partir de la technologie Adxstudio Portals, héberger des formulaires Web (formulaires Web ASP.Net), et permettre les demandes et la réception de services. Le portail sera utilisé par des utilisateurs externes ayant des rôles et des droits bien définis.

(b) **Dynamics CRM (local)** 2015 (ou une version ultérieure)
Technologie de gestion des cas – Le portail offrira une interface avec un outil de gestion des relations avec la clientèle, MS Dynamics CRM (local) 2015 (ou une version plus élevée), en vue d'amorcer des activités de gestion des cas, d'interagir avec de telles activités, de les gérer et de les exécuter. L'outil de gestion des cas est un service géré centralement et servira à des utilisateurs internes dont les rôles et les droits ont été bien définis.

(c) **Serveur Microsoft Exchange, client Outlook**
Système de courriel du GC – Cette technologie servira à donner un accès hors ligne aux utilisateurs internes, notamment aux inspecteurs de chantier.

(d) **Business Objects de SAP**
Établissement de rapports relatifs aux renseignements d'affaires – La suite Business Objects 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 (sur place) 2015 (ou une version ultérieure). Si ceux-ci ne permettent pas l'établissement de rapports stratégiques, la suite Business Objects de SAP connecté à un entrepôt PureData effectuera cette tâche. Les utilisateurs externes aussi bien que les utilisateurs internes doivent avoir accès aux fonctionnalités relatives à l'établissement de rapports.

(e) **Enterprise Service Bus (ESB) d'Oracle**
Technologie de partage de l'information – Plateforme d'interopérabilité du GC (PIGC – fondée sur la technologie de l'Enterprise Service Bus [ESB] d'Oracle). 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 l'Enterprise Service Bus (ESB) d'Oracle.

INSÉRER :

La solution doit tirer parti de la technologie identifiée par TPSGC dans la liste descriptive ci-dessous. Ces technologies sur les suites Enterprise IT Target Suites qui sont pilotées par les directions générales de l'agent d'information (DGDPI) du SCT ou de TPSGC afin de réduire et rationaliser l'empreinte de la demande pour les applications GC et SPAC. Lors possible l'entrepreneur doit satisfaire aux exigences de la solution, y compris toutes les nouvelles exigences axées sur la restructuration des processus métier en utilisant ces technologies pour créer une solution unifiée.

Les suites identifiées auxquelles l'entrepreneur doit adhérer comprennent, sans s'y limiter:

(a) **Dynamics CRM (sur site) 2015 (ou supérieur) (Enterprise IT Target Suite)**
Technologie de gestion des cas - Le portail Web interagira avec un outil de gestion de la relation client, MS Dynamics CRM (sur place) 2015 (ou supérieur), pour initier, interagir, gérer et effectuer des activités de gestion de cas. L'outil de gestion des cas est un service centralisé et sera utilisé par les utilisateurs internes ayant des rôles et des droits définis.

(b) **Serveur Microsoft Exchange, Client Outlook *(Enterprise IT Target Suite*) et MS Dynamics CRM pour le courriel Outlook GC** – Cette technologie sera utilisée afin de supporter les

capacités de gestion de cas par courriel et hors ligne pour les utilisateurs internes, tels que les inspecteurs de terrain.

(c) Objets d'affaires SAP *(Enterprise IT Target Suite)*
Rapports en intelligence d'affaires- Objets d'affaires SAP est la suite d'entreprise pour les analyses d'affaires. Cependant, pour cette solution, les fonctionnalités, y compris les tableaux de bord internes d'utilisateurs, tireront les fonctionnalités de rapport fournies avec les outils Dynamics CRM 2015 (ou supérieur) pour fournir la fonction de rapport opérationnel. Les fonctionnalités de rapport stratégique, si elles ne sont pas disponibles avec Dynamics CRM 2015 (ou supérieur), seront fournies à travers la suite standard Objets d'affaires SAP **c**onnectée à un entrepôt *PureData*. La fonction de rapport doit être disponible pour les utilisateurs internes et externes en fonction des profils d'application des utilisateurs.

(d) *Oracle Service Bus (Enterprise IT Target Suite)* Technologie d'échange d'information - Plate-forme d'interopérabilité GC (GCIP – basé sur *Oracle Service Bus* (technologie). Le partage d'informations entre SSI et les organisations partenaires devrait être automatisé et géré conformément aux capacités GCIP et à la technologie sous-jacente *Oracle Service Bus*.

L'accès contrôlé pour les utilisateurs externes se fera par une interface Internet basée sur l'utilisateur. Le portail Web doit être développé sous la forme d'un portail client CRM basé sur une technologie de portail COTS (sur site) et doit héberger des formulaires compatibles avec le Web pour la réquisition et la réception des services. Le portail Internet sera utilisé par des utilisateurs externes avec des rôles et des droits définis. L'Entrepreneur fournira et configurera une technologie qui réside sur le réseau du GC, qui se connecte parfaitement avec l'application Dynamics CRM, évolutive pour répondre à la taille de l'utilisateur cible, utiliser les services Web et utiliser principalement la configuration sur la personnalisation. Le portail Web configuré doit répondre aux exigences GC (WCAG) pour les normes Web.

Changement 33 :

À la partie 3, 1.1 Exigence Aperçu:

INSÉRER :

(e) Système d'imagerie et de numérisation - Le système est en place et utilise la technologie Datacap d'IBM. La solution de TSSI devra pouvoir échanger de l'information avec le système.

(f) Système de gestion des documents et des dossiers - La solution devra permettre le stockage, la gestion et l'extraction de données provenant des deux catégories suivantes : (1) Base de données ou système de gestion de données – données structurées de transactions de niveau élevé nécessitant un traitement intensif, généralement associées aux demandes en cours et aux données de l'entreprise et du personnel; (2) Système de gestion des documents et des dossiers – données non structurées de transactions de bas niveau dont le traitement d'extraction est peu fréquent, généralement associées aux pièces jointes qui ne doivent pas être modifiées, mais doivent être conservées à des fins de preuve et de gestion des documents et des dossiers (p. ex. passeport, acte de naissance, etc.).

i) **Base de données ou système de gestion de données -** L'entrepreneur peut proposer des solutions en tirant parti des produits existants, déjà sous licence, utilisés par SPAC afin de répondre aux exigences en matière de traitement des données et des renseignements sensibles, non sensibles et circonstanciés. La solution doit respecter les normes de GC établies pour SQL Server et Oracle pour toute application de la base de données.

ii) **Système de gestion des documents et des dossiers -** La norme actuelle au GC en matière de gestion des documents et des dossiers est le serveur de contenu OpenText, lequel devrait être exploité pour le stockage à long terme de données non structurées. Il s'agirait de la configuration par défaut pour les éléments qui ne sont pas nécessaires au traitement dynamique et qui comprennent, sans toutefois s'y limiter, des pièces jointes statiques et des formulaires remplis à la main qui sont numérisés aux fins de gestion des documents et des dossiers.

Changement 34 :

À l'ANNEXE A, partie 3, 1.2 Exigences Techniques :

SUPPRIMER Tech.12 au complet et le **REMPLACER** avec :

Tech.12	Utilise une technologie de portail Web COTS, pour créer un portail Web, des formulaires compatibles avec le Web pour rassembler et échanger des informations à partir du portail Web, est intégré aux entités MS-Dynamics CRM 2015 (ou plus tard) et prend en charge Tech.14 et Tech.18.

Changement 35 :

À l'ANNEXE A, partie 3, 1.2 Exigences Techniques :

SUPPRIMER Tech.17 au complet et le **REMPLACER** avec :

Tech.17	Satisfait à un minimum, les exigences de profil de sécurité "Protégé B, intégrité haute, disponibilité moyenne" (PB / H / M).

Changement 36 :

À l'ANNEXE A, partie 3, 1.2 Exigences Techniques :

SUPPRIMER Tech.18 au complet et le **REMPLACER** avec :

Tech.18	Assure la conformité aux normes Web du GC (https://recherche-search.gc.ca/rGs/s_r?st=s&s5bm3ts21rch=x&num=10&st1rt=0&cdn=canada&hq=&q=normes+web&langs=fra) et aux exigences d'accessibilité Web (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601) pour le portail Web COTS

Changement 37 :

À l'ANNEXE A, partie 4, sous 1.2.1 Utilisateurs internes :

SUPPRIMER :

SécurInt.05	Faire en sorte que l'utilisateur puisse accéder au Système partagé de gestion des cas (SPGC) au moyen d'un réseau privé virtuel (RPV).

INSÉRER :

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).

Changement 38 :

À l'ANNEXE A, partie 5, sous 1.1.2 Catalogue des contrôles de sécurité :

SUPPRIMER :

Voici une description très générale tirée du catalogue des contrôles de sécurité Conseil en matière de sécurité des technologies de l'information nº 33 (ITSG-33), divisé en classes et en familles de contrôle. Ces familles de contrôle s'appliquent aux exigences de sécurité du SSI. Elles sont présentées en partie dans les exigences détaillées dont fait état la présente annexe. Les contrôles couvrant la totalité de la solution se trouvent intégrés aux mises en œuvre techniques existantes, dont le Système partagé de gestion des cas (SPGC). Puisque l'ensemble de la solution constituera principalement un exercice d'intégration, la suite complète de contrôles qui s'y rattache sera évaluée tout au long du développement de la solution au moyen du processus d'évaluation de la sécurité et d'autorisation. Ces familles de contrôle sont le fondement de la sécurité de la solution et de ses données.

INSÉRER :

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.

Changement 39 :

À l'ANNEXE A, partie 5, sous 1.2 Exigences détaillées :

SUPPRIMER :

Les exigences faisant l'objet du tableau qui suit ont été établies suivant un profil Protégé B, intégrité et disponibilité moyennes (PB/M/M), à partir du document ITSG-33. Bon nombre des contrôles qui figurent dans ce document se recoupent ou renvoient les uns aux autres. Les exigences présentées ici correspondent en bonne partie à celles du profil PB/M/M. En sont exclus les éléments dont on s'attend à ce qu'ils soient pris en charge par TPSGC même au moyen de technologies existantes, plutôt que par le SSI ou la présente solution en particulier. La version définitive de la matrice de traçabilité des exigences relatives à la sécurité comportera la liste des contrôles nécessaires au soutien de la solution du SSI. Le contenu du tableau qui suit n'est pas exhaustif et pourrait évoluer durant la période du contrat.

INSÉRER :

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.

Changement 40 :

À l'ANNEXE A, partie 5, sous 1.2 Exigences détaillées :

SUPPRIMER SC.15 au complet et le **REMPLACER** avec :

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.

Changement 41 :

À l'ANNEXE A, partie 5, sous 1.2 Exigences détaillées :

SUPPRIMER SC.28 au complet et le **REMPLACER** avec :

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.

Changement 42 :

À l'ANNEXE A, partie 5, sous 1.2 Exigences détaillées :

SUPPRIMER SC.41 au complet et le **REMPLACER** avec :

SC.41	La solution doit, à tout le moins, satisfaire aux exigences pour PB/H/M.

Changement 43 :

À l'ANNEXE A, partie 7, sous 1.3 Exigences détaillées – Gestion de projet, article PM.04 :

INSÉRER :

(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 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.

Changement 44 :

SUPPRIMER l'ANNEXE C - LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ au complet, et le **REMPLACER** avec l'ANNEXE C - LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ ci-jointe.

Changement 45 :

À ANNEXE F - Information sur la catégorie de ressource pour les services facultatifs, 3.9.2 Qualifications minimales obligatoires :

SUPPRIMER M4 au complet et le **REMPLACER** avec ce qui suit :

M4	Doit avoir au moins trois (3) années d'expérience, au cours des dix (10) dernières années, en développant une livraison de services en ligne utilisant les technologies Web.

B. Questions

Question 10 :

L'État pourrait-il confirmer que tous les travaux associés au projet doivent être ou seront réalisés dans les bureaux du gouvernement?

Réponse 10 :

L'État confirme que tous les travaux associés au projet doivent être réalisés au sein d'une installation du gouvernement. On s'attend à ce que le gestionnaire principal de la prestation de services ou le gestionnaire de projet ainsi que l'équipe de gestion de projet (voir ANNEXE A, partie 7) doivent se trouver sur les lieux et être à la disposition du responsable du projet, au besoin, pour participer aux réunions, présenter des mises à jour, répondre aux préoccupations, etc.

Comme il est indiqué dans la LVERS, partie C, l'entrepreneur ne recevra pas, ne stockera pas et n'utilisera pas ses propres systèmes informatiques pour traiter ou stocker des renseignements ou des biens PROTÉGÉS ou CLASSIFIÉS. En outre, l'entrepreneur ne disposera pas d'un lien électronique entre ses systèmes informatiques et ceux du ministère, en l'occurrence TPSGC.

Ainsi, tous les travaux liés au projet dans le cadre desquels une personne doit avoir un accès direct aux renseignements et aux biens du SSI devront être effectués sur place, pour la durée des travaux. À la suite de l'achèvement des travaux visés, il n'est plus nécessaire que ces ressources soient sur place. Tous les travaux liés au projet n'exigeant pas un accès direct aux renseignements et aux biens du SSI peuvent être réalisés ailleurs. Pour préciser l'emplacement des travaux, des exigences supplémentaires ont été ajoutées à l'ANNEXE 7, partie 7, PM.04. Veuillez vous reporter au changement 43 de la présente modification.

Question 11 :

L'État pourrait-il préciser si les renseignements personnels issus de l'Union européenne et pouvant se soumettre au Règlement général sur la protection des données (RGPD) font partie d'une quelconque façon de la solution?

Réponse 11 :

La solution ne contiendra et ne prendra en charge aucun renseignement assujetti au RGPD.

Question 12 :

La DP indique que l'entrepreneur et la solution doivent observer les lois fédérales, les règles, les politiques, les directives, les normes et les lignes directrices pertinentes, notamment celles décrites dans l'appendice 4 de l'annexe A. Il est possible que l'entrepreneur ignore les modifications apportées aux lois ou les changements aux politiques si le gouvernement ne le tient pas informé pendant la durée du contrat. Alors, nous suggérons que l'État ajoute un énoncé stipulant que « le gouvernement du Canada informera l'entrepreneur des politiques, des directives et des lignes directrices additionnelles, le cas échéant ».

Réponse 12 :

Veuillez vous reporter au changement 20 de la modification 002, où l'énoncé suivant a été ajouté à l'appendice 4 de l'annexe A : « L'autorité du projet informera l'entrepreneur au sujet des lois, des règles, des politiques, des directives, des normes et des lignes directrices fédérales, nouvelles ou modifiées, ayant une incidence sur le projet ».

Question 13 :

La section 1.2.1, Liste des exigences des utilisateurs internes, a deux numéros d'EDT – SecureInt.05. Est-il possible d'attribuer un nouveau numéro à la deuxième exigence de sorte qu'elle suivra la séquence? On lirait alors : SecureInt.06 – Faire en sorte que l'utilisateur puisse accéder au SPGC au moyen d'un RPV.

Réponse 13 :

SecureInt.05 figure deux fois par erreur. Veuillez vous reporter au changement 37 de la présente modification.

Question 14 :

Faut-il présumer que la solution aura accès au système d'essai d'un pair (gouvernement ou autre intervenant) pour que soit testée l'intégration du système?

Réponse 14 :

L'entrepreneur devra décrire en détail toutes les exigences relatives aux essais, dans son plan d'essai. Des environnements seront fournis en fonction de l'approbation de ces plans. L'équipe de projet de TPSGC organisera et coordonnera les essais d'intégration de la solution, à l'interne, de concert avec les partenaires de sécurité (p. ex., la Gendarmerie royale du Canada [GRC], le Service canadien du renseignement de sécurité [SCRS]) et des organisations tierces (p. ex., les agences d'évaluation du crédit). L'entrepreneur sera responsable des aspects détaillés des essais d'intégration, de concert avec les représentants des partenaires de sécurité et des organisations tierces.

Question 15 :

Les exigences obligatoires O1 et O2 mentionnent que « le soumissionnaire doit fournir trois projets de référence comparables à ceux figurant aux sections 2 à 7 de l'annexe A ayant été réalisés dans les quinze années précédant la date de clôture des soumissions et avoir disposé d'un volet d'échange de données avec le public sur Internet ».

Selon notre expérience, nous disposons de projets fédéraux comparables sur l'intranet, qui ont un volume égal ou supérieur à celui nécessaire pour O1 et O2 et qui répondent tout à fait aux autres besoins. Vu que les principaux besoins des projets de référence associés à ERI/GC/GRC, nous croyons qu'il serait suffisant de montrer un élément Web situé sur Internet OU l'intranet pour répondre aux besoins de SPAC.

Nous demandons que les exigences O1 et O2 soient modifiées pour y introduire un « volet d'échange de données avec le public sur Internet ou dans l'intranet ».

Réponse 15 :

À l'heure actuelle, selon les exigences obligatoires O1 et O2 de l'évaluation technique : « Le soumissionnaire doit fournir trois (3) projets de référence ayant été réalisés dans les quinze (15) années précédant la date de clôture des soumissions qui sont similaires aux projets décrits de la partie 2 à la partie 7 de l'ANNEXE A et doivent avoir disposé d'un volet d'échange de données avec le public sur Internet ». Le volet d'échange de données avec le public sur Internet est pertinent, car la solution définitive sera utilisée de la même façon. Ainsi, un projet d'échange de données sur Internet du gouvernement fédéral serait jugé non conforme, car les exigences en matière de sécurité seraient différentes de celles d'un projet d'échange de données avec le public sur Internet.

Question 16 :

L'entrepreneur pourra-t-il réutiliser les canaux actuels d'échange de renseignements pour communiquer avec les partenaires de sécurité de TSSI de SPAC, notamment GRC, SCRS, CSTC, CST, DND et les agences d'évaluation du crédit ou Equifax? Si oui, pourra-t-il présumer que ces canaux répondent aux besoins à l'égard des données actives et inactives du programme TSSI?

Réponse 16 :

L'entrepreneur ne devrait pas supposer que les canaux existants d'échange de renseignements sont conformes à l'architecture proposée, sont conformes aux exigences de sécurité ou sont conformes aux exigences relatives aux processus opérationnels.

Question 17 :

SC.33 – L'entrepreneur doit, pendant la durée du contrat, signaler toutes les atteintes, présumées ou réelles, à la vie privée et à la sécurité comme des incidents de sécurité. Le GC peut-il confirmer ou expliquer la portée de ce point? Ces incidents de sécurité couvrent-ils les événements internes au sein de l'équipe de l'entrepreneur OU l'entrepreneur exercera-t-il une surveillance accrue sur les lieux?

Réponse 17 :

Cette exigence vise simplement à signaler les atteintes réelles à la vie privée et à la sécurité pendant la durée du contrat. Par exemple, si l'entrepreneur soupçonne, est témoin ou a des preuves qu'une personne, un entrepreneur ou autre trafique les données ou la configuration du système, cet incident doit être signalé au GC.

Question 18 :

En référence à l'intégration du centre d'appels **:**

SPAC peut-il confirmer qu'il n'y a aucune intégration entre la technologie du centre d'appels et la solution?

Réponse 18 :

À l'heure actuelle, on n'envisage pas l'intégration de la technologie existante du centre d'appels à la solution.

Question 19 :

En référence à l'Annexe A, partie 2 : Exigences opérationnelles, 2.2 Exigences détaillées – Exigences fonctionnelles, 2.2.1 Application de traitement du service, APP-IM.16 (page 22 de 77);

Parle-t-on seulement d'archivage au sein de la solution ou de la capacité de la solution d'interagir avec la solution d'archivage d'un tiers? Si on parle de la solution d'un tiers, prière de fournir les exigences supplémentaires, comme les spécifications de l'interface, la fréquence, etc.

Réponse 19 :

En ce qui concerne l'ANNEXE A, partie 2, exigence opérationnelle APP-IM.16, on s'attend à ce que l'archivage des dossiers soit réalisé au sein de la solution. Veuillez vous reporter au changement 23 de la présente modification.

Question 20 :

En référence à l'Annexe A, partie 2 : Exigences opérationnelles, 2.2 Exigences détaillées – Exigences fonctionnelles, 2.2.1 Application de traitement du service, APP-IM.27 (page 23 de 77);

Parle-t-on seulement d'archivage au sein de la solution ou de la capacité de la solution d'interagir avec la solution d'archivage d'un tiers? Si on parle de la solution d'un tiers, prière de fournir les exigences supplémentaires, comme les spécifications de l'interface, la fréquence, etc.

Réponse 20 :

En ce qui concerne l'ANNEXE A, partie 2, exigence opérationnelle APP-IM.27, on s'attend à ce que l'archivage des dossiers de cas et l'accès aux dossiers de cas archivés soient réalisés au sein de la solution. APP-IM.27 a été modifié par souci de précision. Veuillez vous reporter au changement 24 de la présente modification.

Question 21 :

En référence à l'Annexe A, partie 2 : Exigences opérationnelles, 2.2 Exigences détaillées – Exigences fonctionnelles, 2.2.1 Application de traitement du service, APP-COM.03 (page 23 de 77) et 2.2.2 Portail de service Web, WP-UE.09 (page 29 de 77);

Le GC fournira-t-il la passerelle SMS? Le cas échéant, prière de fournir les spécifications de l'interface et les contraintes liées à son utilisation.

Réponse 21 :

En ce qui concerne l'ANNEXE A, partie 2, Exigences opérationnelles APP-COM.03 et WP-UE.09, à l'heure actuelle, TPSGC n'a pas de passerelle SMS. Les exigences APP.COM.03 et WP-UE.09 ont été modifiées pour remplacer le terme SMS par messages courriel normalisés. Veuillez vous reporter aux changements 25 et 27 de la présente modification.

Question 22 :

À l'heure actuelle, avez-vous un fournisseur de messagerie texte? Le cas échéant, indiquez le fournisseur.

Réponse 22 :

Veuillez vous reporter à la réponse 21 de la présente modification.

Question 23 :

En référence à l'Annexe A, partie 2 : Exigences opérationnelles, 2.2 Exigences détaillées – Exigences fonctionnelles, 2.2.1 Application de traitement du service, APP-COM.06 (page 23 de 77);
a) **Question :** Comment la correspondance à envoyer par les services postaux sera-t-elle réalisée? La solution doit-elle seulement permettre l'impression, le personnel prenant ensuite la relève, ou un fichier d'interface doit-il être créé et envoyé à un tiers?
b) **Question :** Doit-on tenir compte de volumes et d'un délai précis pour l'achèvement des mesures?

Réponse 23 :

En ce qui concerne l'ANNEXE A, partie 2, Exigence opérationnelle APP-COM.06, la correspondance imprimée sera envoyée manuellement par courriel à TPSGC. À l'heure actuelle, on ne doit tenir compte d'aucun volume ni d'aucun délai précis pour l'achèvement des mesures.

Question 24 :

En référence à l'Annexe A, partie 2 : Exigences opérationnelles, 2.2 Exigences détaillées – Exigences fonctionnelles, 2.2.1 Application de traitement du service, APP-PPL.02 (page 23 de 77);
Parle-t-on uniquement de la capacité d'annexer une image à un dossier de cas?

Réponse 24 :

En ce qui concerne l'ANNEXE A, partie 2 : Exigence opérationnelle APP-PPL.02, il s'agit de la capacité de numériser un document au moyen d'un scanneur externe à la solution et d'annexer le fichier numérisé à un dossier de cas, au sein de la solution. On ne s'attend pas à ce que la solution interagisse avec les scanneurs externes. L'exigence APP-IM.27 de l'ANNEXE A a été modifiée par souci de précision. Veuillez vous reporter au changement 26 de la présente modification.

Question 25 :

En référence à l'Annexe A, partie 2 : Exigences opérationnelles, 2.2 Exigences détaillées – Exigences fonctionnelles, 2.2.1 Application de traitement du service, APP-RP.03 (page 25 de 77);
Recherchez-vous un critère de mesure précis devant être surveillé relatif aux charges de travail individuelles?

Réponse 25 :

En ce qui concerne l'ANNEXE A, partie 2, Exigence opérationnelle APP-RP.03, à l'heure actuelle, il n'existe aucun critère de mesure précis pour surveiller les charges de travail individuelles.

Question 26 :

En référence à l'Annexe A, partie 2 : Exigences opérationnelles, 2.2 Exigences détaillées – Exigences fonctionnelles, 2.2.2 Portail de service Web, WP-RP.01 (page 31 de 77);
Que désignent les « normes du GC »?

Réponse 26 :

En ce qui concerne l'ANNEXE A, partie2, l'exigence opérationnelle WP-RP.01 a été supprimée, car d'autres exigences en matière de production de rapports au sein du volet Portail de service Web de la solution répondront aux besoins opérationnels de TSSI. Veuillez vous reporter au changement 28 de la présente modification.

Question 27 :

En référence aux sections 7.15.2 et 7.15.3 de la DP, TPSGC accepte-t-il de modifier la DP de sorte que la limite de responsabilité décrite à la section 7.15.2(e)(ii) s'applique également aux réclamations, pour les deux parties, et aux dommages causés par une violation des droits de propriété intellectuelle?

Réponse 27 :

TPSGC n'accepte pas de modifier les clauses relatives à la limite de responsabilité figurant à l'article 7.15. Ces clauses sont des clauses standard approuvées par le Conseil du Trésor (CT) élaborées de concert avec l'industrie précisément pour les groupes de produits GI-TI.

Question 28 :

En référence à la section 7.15.2 de la DP, TPSGC accepte-t-il de modifier la DP de sorte que la limite de responsabilité décrite à la section 7.15.2(e)(ii) s'applique également aux manquements de l'entrepreneur de se conformer aux dispositions sur la confidentialité des renseignements personnels, tel qu'il est décrit dans la loi sur la confidentialité applicable?

Réponse 28 :

Veuillez vous reporter à la réponse 27 de la présente modification.

Question 29 :

En référence à la section 7.15.2(e)(ii) de la DP, TPSGC accepte-t-il de remplacer 0,75 par 0,25?

Réponse 29 :

Veuillez vous reporter à la réponse 27 de la présente modification.

Question 30 :

À la section 7.2.1.9, sous Obligation du Canada, la DP indique que le gouvernement du Canada se réserve le droit d'obtenir le travail par d'autres moyens. Elle envisage une refonte importante du processus opérationnel et la mise en œuvre d'un système. Vu que la DP est obtenue grâce à un processus concurrentiel qui permettra au Canada d'évaluer les plans et les approches proposées par le soumissionnaire, nous ne comprenons pas la raison d'une telle exigence, sans compter les clauses de résiliation et les pénalités qui figureront dans les dispositions du contrat. Nous demandons respectueusement le retrait de la référence, qui pourrait être utilisée comme solution à un règlement de différends et comme raison de résilier le contrat, ce qui minerait la relation entre le soumissionnaire et le gouvernement du Canada.

Réponse 30 :

La clause figurant à l'article 7.2.1.9 renvoie à la partie des travaux devant être réalisée, sur demande, dans le cadre du contrat, au moyen d'une autorisation de tâches, comme il est décrit à l'article 7.2 Autorisation de tâches ainsi que dans les sous-articles. Elle ne vise pas à nuire à la relation entre le soumissionnaire et le Canada. Le Canada refuse de modifier la clause, à l'heure actuelle.

Question 31 :

À propos de l'article 7.28 : dans la version provisoire de la DP figure une limite de trois mois pour les services de transition, sans frais à la fin du contrat. Selon la version définitive de la DP, le soumissionnaire doit amorcer les services de transition 12 mois avant la date de fin du contrat, et les fournir pour une période indéterminée. Ce changement expose le soumissionnaire à un risque important, car les clauses de résiliation privilégieront l'État, et aucun plafond ne s'appliquera à l'exigence en question. Selon notre expérience, en raison de ces types de critères, les soumissionnaires devront ajouter des dépenses imprévues dans leur soumission pour se protéger contre les risques potentiels, ce qui aura pour conséquence d'augmenter artificiellement les coûts réclamés au gouvernement. Nous demandons respectueusement le rétablissement du plafond de trois mois dans la DP, à titre de précision et pour protéger le soumissionnaire contre les imprévus qui pourraient augmenter artificiellement les coûts.

Réponse 31 :

Le Canada a modifié l'article 7.28 pour limiter la période des services de transition. Veuillez vous reporter au changement 22 de la présente modification.

Question 32 :

Le texte de la demande de propositions (DP) et la LVERS jointe indiquent que le soumissionnaire peut utiliser des ressources provenant de l'extérieur du Canada (p. ex., l'OTAN).
Étant donné que le système fera la collecte, l'entreposage et le traitement des renseignements délicats, personnels et de base des citoyens canadiens pour des enquêtes de sécurité pouvant être de niveau « très secret », SPAC pourrait-il confirmer qu'il n'a pas l'intention de contraindre les soumissionnaires selon les critères suivants :

a. les soumissionnaires se qualifient à titre d'entreprise canadienne selon la PCIE;
b. les ressources des soumissionnaires (particulièrement celles qui donnent des renseignements techniques, opérationnels et de conception) se limitent aux citoyens canadiens ou à d'autres exclusions pertinentes pour motif de sécurité nationale?

Réponse 32 :

La LVERS fut modifiée avec des changements apportées à la partie A, articles 7b) et 9, pour indiquer que cet approvisionnement est limité au Canada y compris les résidents permanents, et que le fournisseur devra accéder l'information ou les atouts INFOSEC. La partie 7, point 7.4 de la DP, a également été modifiée avec les nouvelles exigences de sécurité liées aux changements ci-dessus, y compris une exigence pour la propriété étrangère et une évaluation de contrôle et d'influence. Voir les changements 21 et 44 dans cette modification.

Question 33 :

Certaines sections de la figure 2 de l'annexe A – Énoncé des travaux sont mises en relief et indiquent « processus d'approvisionnement en cours ».

a. Le terme « processus d'approvisionnement en cours » fait-il allusion à la sollicitation de TSSI de SPAC ou à d'autres processus d'approvisionnement?
b. La mise en œuvre de ces éléments fait-elle partie de la portée de la sollicitation de TSSI de SPAC?
c. Si elle n'en fait PAS partie, quels sont les produits ou les services particuliers qui serviront à mettre en œuvre ces éléments du schéma?
    I. Système d'imagerie/de numérisation
    II. Système de gestion des documents et des dossiers de l'entreprise
    III. Gestion des formulaires

Réponse 33 :

La figure 2 est actuellement en cours d'examen, veuillez vous reporter à la réponse 35 de la présente modification.

Cependant, ce qui suit est toujours applicable pour la Solution.

a. Le terme « processus d'approvisionnement en cours » sera remplacé par « en cours d'élaboration ».

b. L'entrepreneur n'est pas responsable pour la mise en œuvre de ces domaines. L'entrepreneur est responsable pour le développement, l'intégration et toutes les configurations du logiciel, requis pour la création de la solution de TSSI, conformément à l'énoncé des travaux quant à l'utilisation des plateformes technologiques (voir figure 2, annexe A). Par exemple, l'entrepreneur pourra configurer la plateforme du PAPN et ses capacités lorsqu'il définira les spécifications de messagerie requises pour échanger des renseignements avec des organisations partenaires.

c. Conformément à l'énoncé des travaux, l'entrepreneur doit tirer parti des plateformes technologiques (voir figure 2, annexe A) pour configurer, développer et intégrer ces technologies et ainsi mettre au point la solution de TSSI. Ces aspects s'inscrivent dans le projet de configuration de la solution de TSSI, principalement du point de vue de l'intégration.

    i. Système d'imagerie et de numérisation : Le système est en place et utilise la technologie Datacap d'IBM. La solution de TSSI devra pouvoir échanger de l'information avec le système.

    ii. Système de gestion des documents et des dossiers :
    La solution devra permettre le stockage, la gestion et l'extraction de données provenant des deux catégories suivantes : (1) Base de données ou système de gestion de données – données structurées de transactions de niveau élevé nécessitant un traitement intensif, généralement associées aux demandes en cours et aux données de l'entreprise et du personnel; (2) Système

de gestion des documents et des dossiers – données non structurées de transactions de bas niveau dont le traitement d'extraction est peu fréquent, généralement associées aux pièces jointes qui ne doivent pas être modifiées, mais doivent être conservées à des fins de preuve et de gestion des documents et des dossiers (p. ex. passeport, acte de naissance, etc.).

Base de données ou système de gestion de données
L'entrepreneur peut proposer des solutions en tirant parti des produits existants, déjà sous licence, utilisés par SPAC afin de répondre aux exigences en matière de traitement des données et des renseignements sensibles, non sensibles et circonstanciés. La solution doit respecter les normes de GC établies pour SQL Server et Oracle pour toute application de la base de données.

Système de gestion des documents et des dossiers
La norme actuelle au GC en matière de gestion des documents et des dossiers est le serveur de contenu OpenText, lequel devrait être exploité pour le stockage à long terme de données non structurées. Il s'agirait de la configuration par défaut pour les éléments qui ne sont pas nécessaires au traitement dynamique et qui comprennent, sans toutefois s'y limiter, des pièces jointes statiques et des formulaires remplis à la main qui sont numérisés aux fins de gestion des documents et des dossiers.

iii. Gestion des formulaires: les formulaires sont créés à l'aide de produits Adobe, mais l'entrepreneur n'est pas responsable de la création de formulaire. Il existe deux scénarios concernant les formulaires:

1. Les utilisateurs peuvent compléter leur formulaire en utilisant le portail Web, mais au lieu de se soumettre électroniquement, ils choisissent de l'imprimer. La sortie résultante devrait être un document pdf en mode lecture avec un code à barres qui peut être numérisé dès la réception au SSI pour l'entrée et le traitement.
2. Dans le cadre du plan de continuité de l'activité du SSI, si le système est en panne, les utilisateurs pourraient télécharger un pdf à remplir et compléter, et le soumettre au SSI. Un code à barres pour le pdf sera créer, semblable au scénario 1, qui serait numérisé dès la réception au SSI pour la saisie.

Le Canada ne cherche pas la solution pour créer ces pdf à remplir.

Veuillez vous reporter au changement 33 de la présente modification.

Question 34 :

Une des exigences obligatoires fait référence à une politique du SCT pour la productivité de bureau citant la suite Microsoft comme raison pour l'exigence, et semble inclure ADX Studio dans cette suite. Par contre, ADX Studio ne faisait pas partie de la suite de logiciel de bureau original puisque Microsoft n'avait pas acquis la compagnie à la date de remise.

Quel est le raisonnement pour l'inclusion d'ADXstudio et est-ce que la Couronne modifiera l'énoncé de travail pour permettre à d'autres technologies de portail web d'être prises en considération?

Réponse 34 :

La base de l'inclusion de StudioADX était qu'il satisfaisait aux exigences d'intégration de la compatibilité du plate-forme et de la gestion des cas pour la solution. Le Canada envisagera l'utilisation de d'autres technologies de portail Web commerciales proposées (COTS), à condition qu'elles répondent aux exigences de la solution. L'EDT sera modifié pour refléter le retrait de StudioADX en tant que technologie de portail Web COTS. Veuillez vous reporter aux changements 31, 32, 34, 36, et 45 de la présente modification. Des exigences supplémentaires pour un portail Web COTS seront fournies dans une modification future.

Question 35 :

Problème : La DP renvoie à un ensemble important et exhaustif de normes et de politiques relatives à la sécurité et à la protection des renseignements personnels. Ce document comporte également différentes exigences relatives à la sécurité, notamment une exigence générale et imprécise visant la conformité au profil Protégé B moyen-moyen (document ITSG-33 de la CSTC). Or, ce profil compte 428 contrôles et sous-contrôles, qui, dans un grand nombre de cas, dépassent la portée de la DP.

Risque/incidence : Le plus grand risque pour un soumissionnaire est de présenter une proposition de services lorsque la portée n'est pas bien définie et que les coûts peuvent varier grandement. À moins que les exigences exactes relatives à la sécurité (et au contrôle de la sécurité) soient précisées, le soumissionnaire et SPAC pourraient faire face à des risques importants en ce qui a trait aux coûts, aux efforts et au calendrier.

Recommandation : Il est fortement recommandé que SPAC précise à quelles exigences relatives à la sécurité exactement le soumissionnaire doit satisfaire pour assurer une exécution réussie, notamment les contrôles applicables du profil ITSG-33 (comme les contrôles choisis dans la colonne des projets en TI), dont la responsabilité incombe non seulement au soumissionnaire, mais aussi au Canada à titre d'hôte et d'exploitant de la capacité fournie.

Réponse 35 :

Dans le cadre de l'examen continu des besoins opérationnels en matière de sécurité, il a été déterminé que le profil de sécurité approprié pour la solution est Protégé B, intégrité élevée et disponibilité moyenne (PB/E/M). Cela représente un changement par rapport au profil de sécurité actuel indiqué dans l'EDT. Par conséquent, des contrôles de sécurité supplémentaires doivent être appliqués à la solution. Ces contrôles de sécurité supplémentaires sont fournis à des fins de référence en pièce jointe à la présente modification. Toutefois, les nouvelles exigences relatives à la sécurité découlant de la modification du profil de sécurité ainsi que les nouveaux contrôles seront fournis dans une prochaine modification à la Section 5. Veuillez prendre note que les contrôles de l'ITSG-33 ne seront pas tous mis en œuvre par l'entrepreneur. Il est à noter que plusieurs des technologies à intégrer sont mises en œuvre et ont des contrôles de sécurité en place. De même, les contrôles/exigences de sécurité pertinents pour l'infrastructure seront mis en œuvre par Services partagés Canada. L'EDT contient seulement les exigences qui nécessitent des efforts de la part de l'entrepreneur. Il est également à noter que, pendant la période du contrat et compte tenu que l'architecture est davantage développée, un processus d'évaluation et d'autorisation de sécurité (Veuillez vous reporter à Partie 5: Exigences relatives à la sécurité de la TI, 1.1.1 Processus d'évaluation de la sécurité et d'autorisation) des contrôles de sécurité pourrait être requis ou recommandé. Veuillez vous reporter aux changements 29, 30, 35, 39, 40, 41 et 42 de la présente modification pour connaître les changements apportés au profil de sécurité de la solution. De plus, veuillez consulter le document « Contrôles de sécurité supplémentaires », fourni en tant que pièce jointe à la présente modification.

Question 36 :

L'annexe A – Énoncé des travaux, SECTION 5 : EXIGENCES EN MATIÈRE DE SÉCURITÉ DE LA TI, 1.2 EXIGENCES DÉTAILLÉES, SC.41 introduit l'ensemble du Protégé B avec contrôle moyen voulu dans ITSG-33. Plusieurs contrôles semblent surpasser de beaucoup la portée de la demande de propositions (ex. : réseau, COS, surveillance et GIIS).
SPAC pourrait-il indiquer les contrôles qui sont de la responsabilité du soumissionnaire, et lesquels sont du ressort du gouvernement du Canada?

Réponse 36 :

Veuillez vous reporter à la réponse 35 de la présente modification.

Question 37 :

L'architecture conceptuelle énoncée à la section 3, paragraphe 1.1, fait état de la version du Système de gestion de cas partagé (SGCP) de MS Dynamics CRM comme étant la solution de gestion de cas requise. Le paragraphe qui suit celui sur l'architecture conceptuelle ne fait pas état précisément du SGCP, mais indique MS Dynamics CRM 2015 comme étant la technologie de gestion de cas prévue pour la solution. L'État pourrait-il préciser si Microsoft Dynamics CRM 2015, ou la version du SGCP de MS Dynamics, est la plateforme prévue pour la solution CRM?

Réponse 37 :

TPSGC a normalisé l'utilisation de Microsoft Dynamics CRM 2015 (ou une version ultérieure) à titre de plateforme de développement pour les applications de gestion de cas. Il s'agit de la plateforme requise pour la solution de transformation des systèmes de sécurité industrielle (TSSI). La version du SGCP de Microsoft Dynamics CRM, y compris les fonctions et normes connexes, doit être exploité dès que possible et sera mise à la disposition de l'entrepreneur afin qu'il puisse déterminer les éléments de la solution où elle peut s'appliquer. Une modification a été faite pour remplacer les références à SCMS avec Microsoft Dynamics CRM. Veuillez vous reporter aux changements 37 et 38 de la présente modification.

.

TOUTES LES AUTRES MODALITÉS DEMEURENT INCHANGÉES.

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EP243-17-0549 (Rev #3)
Security Classification / Classification de sécurité
Unclassified

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Public Services and Procurement Canada	Departmental Oversight Branch

3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work - Brève description du travail

Industrial Security Systems Transformation Project
The objective of this procurement is to acquire System Integration Services in support of project delivery

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui

6. Indicate the type of access required - Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p.ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciales sans entreposage de nuit?	☑ No / Non	☐ Yes / Oui

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

Canada	NATO / OTAN	Foreign / Étranger
☑	☑	☐

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

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

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

Canada	NATO / OTAN	Foreign / Étranger
☑ PROTECTED A / PROTÉGÉ A	☑ NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	☐ PROTECTED A / PROTÉGÉ A
☑ PROTECTED B / PROTÉGÉ B	☑ NATO RESTRICTED / NATO DIFFUSION RESTREINTE	☐ PROTECTED B / PROTÉGÉ B
☐ PROTECTED C / PROTÉGÉ C	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ PROTECTED C / PROTÉGÉ C
☐ CONFIDENTIAL / CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ CONFIDENTIAL / CONFIDENTIEL
☐ SECRET / SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET	☐ SECRET / SECRET
☐ TOP SECRET / TRÈS SECRET		☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)		☐ TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EP243-17-0549 (Rev #3)
Security Classification / Classification de sécurité
Unclassified

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

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

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :

Document Number / Numéro du document :

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

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

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

Special comments: / Commentaires spéciaux : See attached Security Specification Guide

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

10. b) May unscreened personnel be used for portions of the work? — ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted: — ☑ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	Confidential / Confidentiel	Secret	Top Secret / Très Secret	NATO Restricted / NATO Diffusion Restreinte	NATO Confidential / NATO Confidentiel	NATO Secret	COSMIC Top Secret / COSMIC Très Secret	Protected / Protégé A	Protected / Protégé B	Protected / Protégé C	Confidential / Confidentiel	Secret	Top Secret / Très Secret
Information / Assets / Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Contrôles de sécurité supplémentaires

Note: La description des contrôles est basée sur la version du 30 Décembre 2014 de l'Annexe 3A du guide ITSG-33, Catalogue de contrôles de sécurité.

R=Responsable, S=**S**outien

Famille	Iden. Contrôle	Amélioration	Nom	Classe	Description	Conseils supplémentaires	Fonction STI	Opérations TI	Projets TI	Securité Physique	Sécurité du pers.	Formation	Conseils généraux sur l'adaptation et la mise en œuvre
AC	2	(11)	GESTION DES COMPTES	Technique	GESTION DES COMPTES | CONDITIONS D'UTILISATION Le système d'information applique [Affectation : circonstances et/ou conditions d'utilisation définies par l'organisation] aux [Affectation : comptes du système d'information définis par l'organisation].	Les organisations peuvent décrire les conditions ou les circonstances particulières selon lesquelles les comptes du système d'information peuvent être utilisés, par exemple en limitant l'utilisation à certains jours de la semaine, à certaines heures du jour ou à une durée précise.		S	R				Le contrôle ou l'amélioration offrent une capacité très spécialisée ou évoluée non requise pour tous les systèmes. Leur inclusion dans un profil ministériel relève donc du cas par cas.

AC	10		CONTRÔLE DE SESSIONS SIMULTANÉES	Technique	(A) Le système d'information limite le nombre de sessions simultanées pour chaque [Affectation : type de compte et/ou compte défini par l'organisation] à [Affectation : nombre défini par l'organisation].	Les organisations peuvent définir le nombre maximal de sessions simultanées pour les comptes de système d'information globalement, par type de compte (p. ex. utilisateur privilégié, utilisateur non privilégié, domaine, application précise), par compte ou selon une combinaison. Par exemple, les organisations peuvent limiter le nombre de sessions simultanées pour les administrateurs système ou les utilisateurs travaillant dans des domaines particulièrement sensibles ou avec des applications essentielles à la mission. Ce contrôle concerne les sessions simultanées de comptes de système d'information et non celles effectuées par un seul utilisateur se servant de plusieurs comptes système	S		R				
AU	3	(2)	CONTENU DES ENREGISTREMENTS DE VÉRIFICATION	Technique	CONTENU DES ENREGISTREMENTS DE VÉRIFICATION | GESTION CENTRALISÉE DU CONTENU DE L'ENREGISTREMENT DE VÉRIFICATION PRÉVU Le système d'information centralise la gestion et la configuration du contenu des enregistrements de vérification générés par [Affectation : composants de système d'information définis par l'organisation].	Cette amélioration exige la configuration centralisée du contenu des enregistrements de vérifications (automatisation nécessaire). Les organisations coordonnent la sélection du contenu d'enregistrement requis pour appuyer la capacité de gestion et de configuration centralisée qu'offre le système d'information. Contrôles connexes : AU-6, AU-7.	S	R	S				Le contrôle ou l'amélioration ne peuvent pas être appliqués au moyen de composants commerciaux. La mise en œuvre de ce contrôle ou de cette amélioration peut donc s'avérer quelque peu problématique.

AU	5	(2)	INTERVENTION EN CAS D'ÉCHECS DE VÉRIFICATION	Technique	INTERVENTION EN CAS D'ÉCHEC DE VÉRIFICATION | ALERTES EN TEMPS RÉEL Le système d'information avertit [Affectation : liste des employés, des fonctions ou des emplacements définie par l'organisation] en [Affectation : période en temps réel définie par l'organisation] lorsque les événements d'échec de vérification suivants se produisent : [Affectation : événements d'échec de vérification définis par l'organisation qui nécessitent une alerte en temps réel].	Les alertes génèrent des messages d'urgence pour les organisations. La vitesse à laquelle ces messages sont générés à la suite des alertes en temps réel dépend de la technologie de l'information utilisée (le temps qui s'écoule entre la détection de l'événement et de l'alerte est inférieur à quelques secondes).	S		R				

AU	10		NON-RÉPUDIATION	Technique	(A) Le système d'information offre une protection contre quiconque (ou contre tout processus exécuté en son nom) nie faussement avoir effectué [Affectation : opérations de non-répudiation définies par l'organisation].	La création d'information, l'envoi et la réception de messages et l'approbation d'information (p. ex. confirmation d'un accord ou signature d'un contrat) sont des exemples d'opérations de non répudiation effectuées par des personnes. La non-répudiation protège les personnes contre toute déclaration ultérieure (i) d'un auteur qui nie être le créateur d'un document particulier, (ii) d'un émetteur qui nie avoir transmis un message, (iii) d'un destinataire qui nie avoir reçu un message ou (iv) d'un signataire qui nie avoir signé un document. Les services de non-répudiation peuvent servir à déterminer si l'information provient d'une personne en particulier, si une personne a pris des mesures particulières (p. ex. envoi d'un courriel, signature d'un contrat, approbation d'une demande d'approvisionnement) ou si elle a reçu certains renseignements. Les organisations obtiennent des services de non-répudiation grâce à plusieurs techniques ou mécanismes (p. ex. signatures numériques, reçus numériques de message). Contrôles connexes : SC-12, SC-8, SC-13, SC-16, SC 17, SC-23			R				Le contrôle ou l'amélioration offrent une capacité très spécialisée ou évoluée non requise pour tous les systèmes. Leur inclusion dans un profil ministériel relève donc du cas par cas.

AU	12	(3)	GÉNÉRATION D'ENREGISTREMENTS DE VÉRIFICATION	Technique	GÉNÉRATION D'ENREGISTREMENTS DE VÉRIFICATION | MODIFICATIONS PAR DES PERSONNES AUTORISÉES Le système d'information permet à [Affectation : liste des personnes ou des rôles définie par l'organisation] de modifier la vérification à effectuer sur [Affectation : composants de système d'information définis par l'organisation] en fonction de [Affectation : critères d'événement sélectionnables définis par l'organisation] en dedans de [Affectation : laps de temps défini par l'organisation].	Cette amélioration permet aux organisations d'accroître ou de limiter leurs activités de vérification au besoin pour répondre aux exigences organisationnelles. Il est possible d'accroître les activités de vérification qui sont limitées pour préserver les ressources du système d'information afin de répondre à certaines situations de menace. Les activités de vérification peuvent aussi au contraire être limitées à un ensemble précis d'événements afin de faciliter la réduction des vérifications ainsi que l'analyse et les rapports de vérification. Les organisations peuvent déterminer la durée pendant laquelle les opérations de vérification sont modifiées, par exemple en temps quasi réel, en quelques minutes ou en quelques heures. Contrôle connexe : AU-7			R				
CM	2	(3)	CONFIGURATION DE RÉFÉRENCE	Opérationnelle	CONFIGURATION DE RÉFÉRENCE | CONSERVATION DES CONFIGURATIONS ANTÉRIEURES L'organisation conserve [Affectation : versions de configuration de référence antérieures du système d'information définies par l'organisation] pour permettre le retour à la version précédente.	Pour permettre le retour à des versions antérieures, on peut par exemple conserver des versions de configuration de référence précédentes de matériel, de logiciels, de micrologiciels de même que de fichiers et de données de configuration.		R	0				

CM	3	(1)	CONTRÔLE DES CHANGEMENTS DE CONFIGURATION	Opérationnelle	CONTRÔLE DES CHANGEMENTS DE CONFIGURATION | AUTOMATISATION CONCERNANT LA DOCUMENTATION, LES AVIS ET LES INTERDICTIONS DE CHANGEMENTS L'organisation emploie des mécanismes automatisés dans les cas suivants : (a) documenter les changements proposés au système d'information; (b) aviser [Affectation : autorités d'approbation définies par l'organisation] des changements proposés au système d'information et des demandes de changement approuvées; (c) souligner les changements proposés au système d'information qui n'ont pas été approuvés ou qui ont été jugés défavorables avant [Affectation : période définie par l'organisation]; (d) interdire tout changement au système d'information jusqu'à l'obtention des approbations requises; (e) documenter tous les changements proposés au système d'information; (f) aviser [Affectation : liste des employés définie par l'organisation] des changements au système d'information approuvés.		S	R	S				Le contrôle ou l'amélioration indiquent d'utiliser un mécanisme automatisé. Malgré les avantages évidents qu'offre ce type de mécanisme, le recours à un mécanisme manuel sera suffisant dans la plupart des cas.

CM	7	(2)	FONCTIONNALITÉ MINIMALE	Opérationnelle	FONCTIONNALITÉ MINIMALE | PRÉVENTION DE L'EXÉCUTION DES PROGRAMMES Le système d'information empêche l'exécution des programmes conformément à [Sélection (un choix ou plus) : [Affectation : politiques sur l'utilisation de programmes logiciels et restrictions connexes définies par l'organisation]; règles d'autorisation des modalités d'utilisation d'un programme].	Contrôle connexe : CM-8.			R				
IA	2	(1)	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	Technique	IDENTIFICATION ET AUTHENTIFICATION | ACCÈS RÉSEAU AUX COMPTES PRIVILÉGIÉS Le système d'information applique l'authentification multifactorielle pour l'accès réseau aux comptes privilégiés.	Contrôle connexe : AC -6.			R				
IA	2	(2)	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	Technique	IDENTIFICATION ET AUTHENTIFICATION | ACCÈS RÉSEAU AUX COMPTES NON PRIVILÉGIÉS Le système d'information applique l'authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.				R				

IA	2	(3)	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	Technique	IDENTIFICATION ET AUTHENTIFICATION | ACCÈS LOCAL AUX COMPTES PRIVILÉGIÉS Le système d'information applique l'authentification multifactorielle pour l'accès local aux comptes privilégiés.	Contrôle connexe : AC -6.			R				On considère que le contrôle ou l'amélioration constituent des contrôles de compensation qui doivent être appliqués seulement lorsque la capacité ne peut pas être prise en charge par un contrôle ou une amélioration de secours. Toutes les activités de gestion doivent être menées dans une zone contrôlée. Le contrôle ou l'amélioration peuvent servir à renforcer la capacité de vérification lorsqu'une EMR a permis de cerner une menace interne.
IA	2	(4)	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	Technique	IDENTIFICATION ET AUTHENTIFICATION | ACCÈS LOCAL AUX COMPTES NON PRIVILÉGIÉS Le système d'information applique l'authentification multifactorielle pour l'accès local aux comptes non privilégiés.				R				

IA	5	(11)	GESTION DES AUTHENTIFIANTS	Technique	GESTION DES AUTHENTIFIANTS | AUTHENTIFICATION PAR JETON MATÉRIEL Pour l'authentification par jeton matériel, le système d'information utilise des mécanismes qui répondent [Affectation : exigences en matière de qualité des jetons définies par l'organisation].	L'authentification par jeton matériel signifie habituellement l'utilisation de jetons d'ICP tels que la carte PIV (Personal Identity Verification) du gouvernement américain. Les organisations définissent certaines exigences précises pour les jetons, dont notamment la compatibilité à une ICP en particulier.	S	S	R				Le contrôle ou l'amélioration offrent une capacité très spécialisée ou évoluée non requise pour tous les systèmes. Leur inclusion dans un profil ministériel relève donc du cas par cas.
IR	4	(1)	TRAITEMENT DES INCIDENTS	Opérationnelle	TRAITEMENT DES INCIDENTS | PROCESSUS AUTOMATISÉS DE TRAITEMENT DES INCIDENTS L'organisation utilise des mécanismes automatisés pour appuyer le processus de traitement des incidents.	Les mécanismes automatisés appuyant les processus de traitement des incidents comprennent notamment les systèmes de gestion des incidents en ligne.	S	R	S				Le contrôle ou l'amélioration indiquent d'utiliser un mécanisme automatisé. Malgré les avantages évidents qu'offre ce type de mécanisme, le recours à un mécanisme manuel sera suffisant dans la plupart des cas.

SA	4	(2)	PROCESSUS D'ACQUISITION	Gestion	PROCESSUS D'ACQUISITION | CONCEPTION / CONTRÔLES DE SÉCURITÉ : RENSEIGNEMENTS RELATIFS À LA MISE EN ŒUVRE L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe fournisse des renseignements sur la conception et la mise en œuvre des contrôles de sécurité à employer, ce qui comprend ce qui suit : [Sélection (une ou plusieurs) : interfaces de systèmes externes ayant trait à la sécurité; conception de haut niveau; conception de bas niveau; code source ou schémas des composants matériels; [Affectation : renseignements produits par l'organisme sur la conception/sur la mise en œuvre]] selon [Affectation : degré de détails définit par l'organisation].	Les organisations pourraient exiger un degré différent de détail concernant la conception et la mise en œuvre des contrôles de sécurité à employer dans les systèmes organisationnels d'information, les composant de systèmes ou les services connexes en fonction des exigences de la mission ou des opérations, des exigences en matière de fiabilité et de résilience, et des exigences en matière d'analyse et de tests. Les systèmes d'information peuvent être partitionnés en plusieurs sous systèmes. Chacun de ces sous systèmes peut également comprendre un ou plusieurs modules. La conception de haut niveau pour les systèmes se traduit par une multiplicité de sous systèmes interreliés par des interfaces qui fournissent des fonctionnalités de sécurité. La conception de bas niveau pour les systèmes se traduit par la création de modules axés sur les logiciels et les microgiciels (sans exclure le côté matériel pour autant) reliés par des interfaces qui fournissent des fonctionnalités de sécurité. Le code source et les schémas de composants matériels sont principalement considérés comme des représentations de la mise en œuvre d'un système d'information. Contrôle connexe : SA 5.	S		R				

SA	4	(9)	PROCESSUS D'ACQUISITION	Gestion	PROCESSUS D'ACQUISITION | FONCTIONS / PORTS / PROTOCOLES / SERVICES UTILISÉS L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe identifie, dès le début du cycle de développement des systèmes, les fonctions, les ports, les protocoles et les services qui seront utilisés dans l'organisation.	L'identification précoce des fonctions, des ports, des protocoles et des services (p. ex. pendant les phases initiales de définition des besoins et de conception) permet aux organisations d'influer sur la modélisation d'un système d'information, de ses composants ou des services connexes. Cette intervention précoce dans le cycle de développement des systèmes permet aux organisations d'éviter ou de réduire au minimum l'utilisation des fonctions, des ports, des protocoles ou des services pouvant poser des risques tout aussi importants qu'inutiles, et de comprendre les avantages de bloquer l'accès à certains ports, protocoles ou services (ou lorsqu'il s'agit de demander à des fournisseurs de services de systèmes d'information de faire de même). Une identification hâtive des fonctions, des ports, des protocoles et des services évite d'avoir à reconfigurer les contrôles de sécurité après la mise en œuvre d'un système d'information, de ses composants ou des services connexes. Le SA 9 décrit les exigences relatives aux services de systèmes d'information externes des organisations, et identifie les fonctions, les ports, les protocoles et les services qui sont fournis depuis des sources externes. Contrôles connexes : CM 7, SA 9.			R				

SC	4		INFORMATION CONTENUE DANS LES RESSOURCES PARTAGÉES	Technique	(A) Le système d'information empêche tout transfert d'information non autorisé et involontaire découlant du partage des ressources du système.	Ce contrôle vise à empêcher l'information (y compris ses représentations chiffrées) produite par les opérations effectuées par des utilisateurs/des rôles antérieurs (ou des processus exécutés en leur nom) d'être transmise à des utilisateurs ou des rôles (ou processus) actuels qui accèdent à des ressources partagées (p. ex. registres, mémoire principale, disques durs) après que ces ressources ont été retournées aux systèmes d'information. Le contrôle de l'information contenue dans les ressources partagées est aussi couramment appelé réutilisation d'un objet et protection de l'information résiduelle. Ce contrôle ne s'applique pas (i) à la rémanence d'information, laquelle désigne les représentations résiduelles de données qui ont été supposément effacées ou supprimées; (ii) ni aux canaux cachés (y compris les canaux de stockage ou de synchronisation) où les ressources partagées sont manipulées de façon à enfreindre les restrictions relatives aux flux d'information, (iii) ni aux composants des systèmes d'information, chacun associé à un seul utilisateur ou un seul rôle. Contrôles connexes : AC 3, AC 4, MP 6			R				On considère que le contrôle ou l'amélioration constituent une pratique exemplaire. Leur inclusion dans un profil ministériel est donc fortement recommandée dans la plupart des cas. Toutefois, ils ne peuvent pas être appliqués au moyen de composants commerciaux. Leur application peut donc s'avérer problématique.

SI	6		VÉRIFICATION DE LA FONCTIONNALITÉ DE SÉCURITÉ	Opérationelle	(A) Le système d'information vérifie l'exploitation correcte de [Affectation : fonctions de sécurité définies par l'organisation]. (B) Le système d'information vérifie le bon fonctionnement des fonctions de sécurité [Sélection (un ou plusieurs): [Affectation : états transitionnels du système définis par l'organisation]; à la demande d'un utilisateur qui possède les privilèges appropriés; [Affectation : période définie par l'organisation]]. (C) Le système d'information avertit [Affectation : personnel ou rôles définis par l'organisation] lorsque des tests de vérification de sécurité sont échoués. (D) Le système d'information [Sélection (un ou plusieurs) : arrête le système; redémarre le système; [Affectation : autre(s) mesure(s) définie(s) par l'organisation]] lorsque des anomalies sont relevées.	Les états transitionnels des systèmes d'information comprennent notamment le démarrage, le redémarrage, l'arrêt et l'interruption. Les notifications fournies par les systèmes d'information comprennent, entre autres, des alertes électroniques à l'intention des administrateurs des systèmes, des messages à l'intention des consoles locales et des indications matérielles, comme des témoins lumineux. Contrôles connexes : CA-7, CM-6	S	R	S				

SI	7	(5)	INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION	Opérationelle	INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | AUTOMATISATION DES INTERVENTIONS EN CAS D'ATTEINTE À L'INTÉGRITÉ Le système d'information [Sélection (un ou plusieurs) : arrête le système; redémarre le système; [Affectation : autre(s) mesure(s) définie(s) par l'organisation]] lorsque des atteintes à l'intégrité sont relevées.	L'organisation peut définir différentes vérifications de l'intégrité et interventions lorsque des anomalies sont relevées : (i) en fonction du type d'information (p. ex. micrologiciel, logiciel, données utilisateur); (ii) en fonction d'informations précises (p. ex. microprogramme de démarrage, microprogramme de démarrage pour un type particulier de machine); ou (iii) une combinaison des deux. La mise en œuvre automatique des mesures de protection comprend, par exemple, le retour en arrière du changement, l'arrêt du système d'information ou le déclenchement d'une alerte de vérification dès qu'un changement non autorisé s'effectue dans un fichier de sécurité essentiel.	S	R	S				