RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Jason Knowles
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Tower C - Office 12C1 - 102-62
jason.knowles@pwgsc-tpsgc.gc.ca
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 956-1418

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet Transformation services courriels	
Solicitation No. - N° de l'invitation 2B0KB-123327/B	**Date** 2012-06-21
Client Reference No. - N° de référence du client 20123327	**GETS Ref. No. - N° de réf. de SEAG** PW-$TSS-002-24571
File No. - N° de dossier 002tss.2B0KB-123327	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2012-07-18**	**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: Knowles, Jason	**Buyer Id - Id de l'acheteur** 002tss
Telephone No. - N° de téléphone (819) 956-1418 ( )	**FAX No. - N° de FAX** (819) 956-5165
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** SHARED SERVICES CANADA AIRPORT PARKWAY DATA CENTRE 700 MONTREAL RD., BLDG C, 8TH FL. OTTAWA Ontario K1A0P7 Canada	

Comments - Commentaires
Exemption au titre de la sécurité nationale : Le processus d'approvisionnement associé à cette initiative est visé par une exception relative à la sécurité nationale et, par conséquent, est exclu de toutes les obligations en vertu des accords commerciaux

Instructions: See Herein

Instructions: Voir aux présentes

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

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

Issuing Office - Bureau de distribution
Data Centre Services/Services des centres de traitement de données
5C2, Place du Portage, Phase III
11 Laurier Street
Gatineau
Québec
K1A 0S5

Canada

Les documents pour cette lettre d'intérêt sont en pièce jointe

Services partagés Canada

Initiative de transformation des services de courriels

Demande de renseignements

Table des matières

Exception relative à la sécurité nationale

Exemption relative à la sécurité nationale : Le processus d'approvisionnement associé à cette initiative est visé par une exception relative à la sécurité nationale et, par conséquent, est exclu de toutes les obligations prévues par les accords commerciaux.

Objet et contenu de la présente demande de renseignements

Le présent document est une demande de renseignements (DDR) liée à l'Initiative de transformation des services de courriels de Services partagés Canada visant à obtenir l'avis de l'industrie sur cette initiative. Le contenu général de la présente demande de renseignements est le suivant :

- **PARTIE I – Processus de DDR :** Renseignements sur l'objet de la présente demande de renseignements et la procédure que l'industrie doit suivre pour y répondre.
- **PARTIE II – Contexte** : Mandat de Services partagés Canada, objectifs opérationnels de l'Initiative de transformation des services de courriels, approche proposée en matière d'approvisionnement, portée et options relatives à la prestation du service.
- **PARTIE III – Exigences obligatoires prévues**: Exigences que les soumissionnaires éventuels devraient respecter selon le Canada.
- **PARTIE IV – Questions** : Questions qui visent à obtenir l'avis de l'industrie et qui permettront au Canada de déterminer l'approche d'approvisionnement ainsi que la stratégie à adopter pour les services de courriels.
- **Annexes A à J** – Données de référence et critères d'évaluation obligatoires et cotés proposés.

PARTIE I : PROCESSUS DE DEMANDE DE RENSEIGNEMENTS

1. INTRODUCTION

Le présent document est une demande de renseignements (DDR) liée à l'Initiative de transformation des services de courriels (ITSC) de Services partagés Canada (SPC), initiative visant à fournir une nouvelle solution de courriel[1] à SPC ainsi qu'aux ministères et organismes auxquels SPC offre des services de technologie de l'information (TI), qui sont appelés « partenaires » de SPC dans le présent document. SPC fournira aussi ce nouveau service aux autres organismes du gouvernement du Canada[2] de manière facultative.

Travaux publics et Services gouvernementaux Canada (TPSGC) et SPC souhaitent obtenir l'avis de l'industrie sur les sujets suivants :

(i) aptitude à répondre aux exigences obligatoires prévues décrites à la partie III;
(ii) questions posées à la partie IV de la présente demande de renseignements;
(iii) Recommandations de l'industrie sur une approche à faible risque que pourrait prendre en considération SPC en vue d'offrir au GC un service de courriel consolidé correspondant aux résultats liés aux opérations, aux échéanciers et à la réductions des coûts mentionnés dans l'ensemble du présent document; et
(iv) aptitude à répondre aux critères d'évaluation (obligatoires et cotés) (provisoires) prévus à l'annexe D.

Le GC souhaite utiliser l'avis obtenu aux points (i) et (ii) pour consolider son approche d'approvisionnement et déterminer la marche à suivre pour l'acquisition, la mise en œuvre et la gestion de la solution de courrier électronique. Il souhaite en outre utiliser l'avis obtenu au point (iii) pour déterminer les critères d'évaluation obligatoires et cotés auxquels les organismes devront répondre à la prochaine étape du processus d'approvisionnement, dans le cadre de laquelle le Canada établira un sous-ensemble de répondants retenus en vue d'étapes ultérieures du processus d'approvisionnement.

1.1 Nature de la présente demande de renseignements

Le présent document n'est pas une demande de soumissions. La demande de renseignements ne donnera pas lieu à l'attribution d'un marché. Par conséquent, les fournisseurs éventuels de biens ou de services décrits dans la demande de renseignements ne doivent pas réserver des stocks ou des installations, ni affecter des ressources en

[1] Une solution de courrier électronique peut être composée d'un ou plusieurs systèmes de TI, réseaux de communication, serveurs, applications serveur et applications client, etc., mis en œuvre, utilisés et gérés dans un environnement du gouvernement du Canada, ou utilisés dans le cadre d'un service offert par un fournisseur de services commerciaux.

[2] Une liste complète des organismes du GC est fournie à http://www.tbs-sct.gc.ca/gov-gouv/tools-outils/org-fra.asp. Les autres organismes gouvernementaux sont ceux mentionnés sur ce site Web qui n'incluent pas SPC et ses partenaires, qui sont énumérés à l'annexe E

fonction des renseignements présentés dans la demande de renseignements. Elle ne donnera pas lieu non plus à la création de listes de fournisseurs. Par conséquent, le fait qu'un fournisseur éventuel de la solution de courriel réponde ou non à la présente DDR ne l'empêchera pas de participer à tout processus d'approvisionnement ultérieur. En outre, la présente demande de renseignements n'entraînera pas nécessairement l'achat de l'un ou de l'autre des biens et des services qui y sont décrits. La DDR vise seulement à obtenir l'avis de l'industrie sur les éléments qui y sont décrits.

2. CONSIGNES À SUIVRE POUR RÉPONDRE À LA DEMANDE DE RENSEIGNEMENTS

2.1 Terminologie

Les termes utilisés dans la présente demande de renseignements sont définis à l'annexe A, Glossaire.

2.2 Coûts associés aux réponses

Le Canada ne remboursera aucuns frais engagés par les organismes pour répondre à la présente DDR.

2.3 Traitement des réponses

Utilisation des réponses : Les réponses ne seront pas soumises à une évaluation officielle. Toutefois, le Canada pourra les utiliser afin d'élaborer ou de modifier l'approche d'approvisionnement et tout document provisoire contenu dans la présente demande de renseignements. Le Canada examinera toutes les réponses reçues d'ici la date de clôture de la demande de renseignements et peut, à sa discrétion, examiner les réponses reçues après cette date**.**
Équipe d'examen : Une équipe d'examen constituée de représentants de SPC et de ses partenaires (le cas échéant) et de TPSGC examinera les réponses. Le Canada se réserve le droit d'embaucher des experts-conseils indépendants ou d'utiliser des ressources de l'appareil gouvernemental, s'il le juge nécessaire, pour l'examen des réponses. Chaque réponse ne sera pas nécessairement examinée par tous les membres de l'équipe d'examinateurs.

Confidentialité : Les répondants devraient indiquer les parties de leur réponse qu'ils jugent de nature exclusive ou confidentielle. Le Canada traitera les réponses selon les dispositions de la *Loi sur l'accès à l'information*.

2.4 Activité de suivi

Le Canada peut, à sa seule discrétion, communiquer avec un répondant pour obtenir des éclaircissements sur les réponses fournies ou pour poser d'autres questions, par écrit ou par l'intermédiaire de réunions individuelles dans le cadre de la DDR, comme le décrit l'avis concernant la journée de consultation de l'industrie dans le cadre de l'ITSC, sur www.merx.com. Le Canada prévoit tenir des réunions individuelles avec certains répondants les 27, 28 et 30 juillet 2012. Ces dates pourraient toutefois changer.

2.5 Contenu de la demande de renseignements

Le présent document est en cours d'élaboration, et il se peut que des clauses ou des exigences soient ajoutées à la demande de soumissions qui sera ultimement publiée par le Canada. Il se peut en outre que des clauses ou des exigences soient supprimées ou modifiées. Les répondants sont invités à faire part de leurs observations concernant un aspect du document provisoire. La demande de renseignements comprend aussi des questions particulières à l'intention de l'industrie.

2.6 Données volumétriques

Les données présentées dans la présente demande de renseignements sont fournies à titre d'information seulement. Bien qu'il s'agisse des meilleurs renseignements dont SPC dispose actuellement, le Canada ne peut garantir ni déclarer que ces données sont complètes, à jour ou exemptes d'erreurs.

2.7 Présentation des réponses

Page de couverture : Si la réponse comporte plusieurs documents, les répondants doivent indiquer sur la page de couverture de chaque document le titre de la réponse, le numéro de la demande de renseignements, le numéro du document et le nom officiel complet du répondant.

Page de titre : La première page de chaque document de la réponse, après la page de couverture, doit être la page de titre, qui doit comporter les éléments suivants :

(i) le titre de la réponse du répondant ainsi que le numéro de volume;

(ii) le nom et l'adresse du répondant;

(iii) le nom, l'adresse et le numéro de téléphone de la personne-ressource du répondant;

(iv) la date;

(v) le numéro de la DDR.

Nombre de copies : Le Canada demande aux répondants de transmettre leur réponse dans un format PDF non protégé, par courriel, à l'adresse suivante : ConsultationSPC.SSCConsultation@tpsgc-pwgsc.gc.ca, si la taille du document est inférieure à 6 Mo. Le Canada demande aussi aux répondants de sauvegarder une copie de leur document PDF (2003 ou version plus récente) sur deux disques compacts (CD-R) ou deux vidéodisques numériques (DVD-R) et d'envoyer les disques par courrier à l'adresse mentionnée à la section 2.8. Le format PDF est requis pour permettre aux répondants d'inclure dans seul un fichier d'autres éléments (tableur, papier blanc, dépliant, etc.) avec leurs documents.

2.8 Demandes de renseignements

Comme il ne s'agit pas d'une invitation à soumissionner, le Canada ne répondra pas nécessairement par écrit et ne distribuera pas forcément les réponses aux répondants.

Toutefois, les répondants qui ont des questions à propos de la présente demande de renseignements peuvent les transmettre à :

Autorité contractante : Jason Knowles

Ministère des Travaux publics et des Services gouvernementaux
Place du Portage III, 12C1
11, rue Laurier
Gatineau (Québec)
K1A 0S5

Adresse courriel : SSCConsultation.ConsultationSPC@tpsgc-pwgsc.gc.ca

Téléphone : 819-956-1418
Télécopieur : 819-956-5165

2.9 Présentation des réponses

Heure et lieu de présentation des réponses : Les organisations qui souhaitent donner une réponse doivent transmettre celle-ci à l'autorité contractante précitée avant le 18 juillet 2012 à 15 h, heure avancée de l'Est.

Responsabilité relative au respect des délais prescrits : Il incombe à chaque répondant de veiller à ce que sa réponse soit transmise à la bonne adresse dans les délais prescrits.

Identification des réponses : Chaque répondant devrait s'assurer que son nom et son adresse, le numéro de la demande et la date de clôture apparaissent clairement sur l'enveloppe de la réponse.

PARTIE II : DONNÉES FONDAMENTALES SUR L'INITIATIVE DE TRANSFORMATION DES SERVICES DE COURRIELS

3. APERÇU DE L'ORGANISME

3.1 Aperçu de Services partagés Canada

La TI est essentielle aux activités quotidiennes du gouvernement fédéral et à la prestation de services aux Canadiens. Dans le passé, tous les ministères et organismes fédéraux utilisaient et géraient leur propre infrastructure de TI, ce qui donnait lieu à une fragmentation des services, à un chevauchement des tâches et à des pertes d'argent.

Pour résoudre ce problème, le gouvernement du Canada a créé Services partagés Canada (SPC) le 4 août 2011 avec, pour mandat, de regrouper les unités organisationnelles des services de centre de données, de courriel et de télécommunications pour les ministères et les organismes cités à l'annexe E[3].

Le SPC a reçu le mandat, conformément au Budget 2011, « d'améliorer l'efficacité et l'efficience des activités et des programmes du gouvernement, afin d'assurer une utilisation optimale de l'argent des contribuables. »[4]

Lors de l'annonce de la création de SPC, Rona Ambrose, ministre de Travaux publics et Services gouvernementaux Canada a déclaré :

> « Services partagés Canada aura pour mandat de rationaliser les services de TI du gouvernement et d'y réduire les chevauchements. Cette initiative aidera notre gouvernement à réduire le chevauchement, et au fil du temps, notre empreinte écologique. Elle permettra également de renforcer la sécurité des données gouvernementales afin d'assurer la protection des Canadiens. [5]
>
> Le passage d'une approche axée sur des solutions coûteuses propres à chaque ministère à une approche pangouvernementale uniformisée nous permettra d'améliorer les services à moindre coût pour la population canadienne. En créant Services partagés Canada, nous nous assurons que les Canadiens et les Canadiennes reçoivent les services de la technologie de l'information les plus efficaces et que leur argent est utilisé de façon responsable. »[6]

SPC normalisera et regroupera toutes les infrastructures actuelles de TI, aidera les organismes liés au centre de données et aux services de courriels et de télécommunications de SPC et de ses partenaires, et fera en sorte que ces services soient fournis à l'ensemble de l'appareil gouvernemental, ce qui amènera une efficience opérationnelle importante et des économies d'échelle.

---

[3] http://www.pco-bcp.gc.ca/oic-ddc.asp?lang=eng&Page=&txtOICID=2011-876&txtFromDate=&txtToDate=&txtPrecis=&txtDepartment=&txtAct=&txtChapterNo=&txtChapterYear=&txtBillNo=&rdoComingIntoForce=&DoSearch=Search+%2F+List&viewattach=24553&blnDisplayFlg=1
(ordonnance du Conseil privé P.C. 2011-876 à P.C. 2011-887, 4 août 2011)

[4] Budget 2011, Prochaine phase du Plan d'action économique du Canada, 6 juin 2011

[5] Rona Ambrose, ministre, Services partagés Canada, 4 août 2011

[6] Ibidem.

En ce qui a trait aux services de courriels, Services partagés Canada a lancé l'Initiative de transformation des services de courriels (ITSC), dont le principal objectif est de remplacer les systèmes de courriel actuels par une solution de courriel regroupée[7] pour le gouvernement du Canada. Cette solution sera mise en œuvre dans chaque ministère et organisme auquel SPC offre des services. SPC fournira ce même service de courriel de manière facultative aux autres ministères et organismes.

3.2 Aperçu du système de courriel à Services partagés Canada

Le courrier électronique, ou courriel, est un élément clé de l'infrastructure de TI. Le courriel est devenu un moyen de communication privilégié pour le gouvernement, que ce soit à l'interne, pour ses activités, ou à l'externe, pour communiquer avec les citoyens canadiens et l'industrie. De par sa nature, le courriel constitue aussi un important environnement de tenue de dossiers, ce qui est essentiel aux opérations gouvernementales.

Bien que le gouvernement fédéral ait mis en place des politiques et des lignes directrices sur l'architecture de TI, un grand nombre d'infrastructures disparates fournissent toujours une multitude de systèmes de courriel. Tous les ministères et organismes partenaires utilisent en général des solutions de courrier électronique possédant différentes versions et différents niveaux de maintenance et de sécurité. Chaque système de courriel a été acheté séparément, puis géré et appuyé par les processus de gestion et les modèles de soutien de TI propres à chaque ministère ou organisme.
Les ministères et organismes partenaires auxquels SPC fournit des services d'infrastructure utilisent donc 63 systèmes de courriel distincts. Bon nombre de ces systèmes ont été mis en œuvre de manière décentralisée, avec des services de courriels présents à des centaines d'endroits. Il faut de plus prendre note que plusieurs de ces systèmes gèrent des renseignements de niveau Classifié à Secret.

À l'échelle de l'organisation, cette mise en œuvre fragmentée représente un environnement complexe, inefficient et coûteux, comme le montrent les faits suivants :

(i) Il n'existe aucune norme sur les courriels à l'échelle du GC.
(ii) On note des problèmes de compatibilité entre les systèmes de courriel du GC.
(iii) À cause de l'exploitation de systèmes de courriel multiples au gouvernement, les ministères et les organismes ont des licences séparées et disposent de leurs propres équipes de soutien technique.

[7] Le mot « regroupé », dans ce contexte, signifie que la solution de l'Initiative de transformation des services de courriels choisie répondra aux exigences de SPC et de ses partenaires en matière de courriels.

Veuillez consulter l’annexe C, Sommaire de l’état actuel, pour en savoir plus sur l’environnement de courriel actuel des partenaires de SPC.

4. FACTEURS ET OBJECTIFS OPÉRATIONNELS

4.1 Facteurs opérationnels

4.1.1 Complexité

Le GC, dans son ensemble, compte des centaines de configurations de systèmes de courriel pour ses employés. Dans les ministères et organismes partenaires, il existe 63 configurations de système de courriel qui comprennent diverses solutions et versions logicielles qui sont exploitées sur des plateformes distinctes et gérées par des organismes de soutien correspondant à chaque ministère et organisme.

À noter :

- Les systèmes de courriel actuels s'accompagnent de nombreux problèmes de compatibilité. En effet, les résultats provisoires démontrent que 81 % des ministères ou organismes utilisent Microsoft Exchange, 13 % Novell GroupWise et 6 % IBM Lotus Notes pour leur système de courriel, alors que les partenaires utilisent des versions différentes et ont adopté des règles et des pratiques également différentes sur l'utilisation des courriels, ce qui entraîne des problèmes d'interopérabilité et des coûts plus élevés.
- Comme de nombreux systèmes de courriel sont utilisés à l'échelle du gouvernement, les ministères et les organismes ont négocié et acquis des licences d'utilisation distinctes et se sont dotés de leurs propres équipes de soutien technique, ce qui entraîne un chevauchement des tâches inutile et onéreux[8].

4.1.2 Pressions financières

Afin de déterminer des occasions d'économie supplémentaires et d'améliorer la prestation de services, le gouvernement du Canada a entrepris, en 2010, le réexamen complet de ses fonctions administratives et de ses frais généraux. [9] Les organismes fédéraux ont été invités à trouver des économies et à réduire leurs dépenses à la lumière des priorités économiques du gouvernement.

Les dépenses de TI du gouvernement du Canada sont estimées à 5 milliards de dollars par année[10] environ, et les possibilités d'économiser sont importantes. Toutefois, dans le modèle fédéré actuel, chaque ministère gère sa propre organisation de TI et acquiert lui-même ses biens et services de TI. De plus, pour répondre à l'attente du gouvernement du Canada concernant des services de haute qualité, sécuritaires et fiables, le coût de la TI augmente constamment.

Le regroupement des systèmes de courriel de SPC et de ses partenaires permet de réduire les frais généraux en éliminant le chevauchement des tâches et en

[8] Ibidem.

[9] Budget 2010, Plan d'action économique du Canada, 4 mars 2010

[10] Étude de faisabilité des centres de données, PricewaterhouseCoopers, 25 avril 2011) (http://www.tpsgc-pwgsc.gc.ca/services/efcd-dcfs/index-fra.html)

rationalisant les opérations. Par ailleurs, dans le contexte précis du courriel, les éléments moteurs de la rationalisation des coûts sont les suivants :

(i) Les mises en œuvre dans chacun des ministères ont donné lieu à des redondances des fonctions de gestion et de soutien pour l'administration des systèmes de courriel. À l'heure actuelle, plus de 400 personnes sont affectées à la gestion des 63 systèmes de courriel actuellement utilisés par les partenaires de SPC (environ 1 700 serveurs de courriel sont nécessaires). Tous ces systèmes nécessitent un approvisionnement en électricité, des services de maintenance, des licences, etc.;

(ii) Si les utilisateurs de systèmes de courriel sont répartis dans tout le Canada, les missions étrangères et d'autres endroits, chaque ministère a établi une architecture différente pour ses services de courriels. Cela a entraîné des chevauchements de réseaux, dont un grand nombre sont non interopérables et, par conséquent, plus coûteux; et,

(iii)Les 1700 serveurs de courriel sont distribués à l'échelle du pays ainsi qu'é l'échelle internationale dans des centres de données de diverses tailles et de divers niveaux d'efficacité, ce qui fait augmenter les coûts et la complexité de la gestion des services de courriels.

4.1.3 Pressions liées à la sécurité

Les Canadiens et les organismes du secteur privé comptent de plus en plus sur des services en ligne pour exercer leurs activités. Le gouvernement doit alors, en retour, interagir avec les Canadiens par l'intermédiaire des voies de communication en ligne. L'utilisation des courriels est donc devenue une méthode prédominante pour interagir avec les Canadiens et les entreprises.

Comme on le sait, le courriel est un vecteur[11] majeur de menaces qui permet de nuire aux réseaux informatiques, et pour mettre en place une solution de courriel générale, il faut renforcer la posture de sécurité afin de résister aux attaques complexes, notamment aux menaces sophistiquées et persistantes (MSP), comme le décrit le document intitulé « Principes de prévention contre les menaces sophistiquées et persistantes » de Sécurité publique Canada[12].

Pour compliquer les choses, la sécurité des systèmes de courriel était ordinairement gérée de manière distincte par chaque ministère ou organisme. Chacun évaluait lui-même les risques relatifs à ses systèmes de courriel et déterminait la façon de mettre en œuvre les mesures et les contrôles de sécurité d'après ses besoins opérationnels. Les agents de sécurité des ministères, de concert avec des experts

[11] Chemin d'accès ou outil qu'un pirate informatique utilise pour accéder à un ordinateur ou à un serveur de réseau pour causer du tort

[12] http://www.securitepublique.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

des TI, déterminaient la façon d'appliquer les mesures et les contrôles de sécurité, conformément à la Politique sur la sécurité du gouvernement[13].

Toutefois, la Politique sur la sécurité du gouvernement n'indique pas comment mettre en œuvre la sécurité des courriels, et les ministères et organismes ont alors utilisé leurs propres normes techniques spécifiées pour répondre à leurs propres exigences, à des niveaux de protection divers. Or, l'utilisation de normes diverses n'assure pas à tous les ministères la même protection contre les menaces liées au courrier électronique.

Enfin, environ 15 000 fonctionnaires fédéraux ont accès à un système de courriel certifié pour la gestion de renseignements de niveau Classifié, jusqu'au niveau Secret inclusivement (y compris Protégé C), et/ou de renseignements protégés, jusqu'au niveau Protégé B inclusivement. Une telle solution est nécessaire pour continuer à soutenir les utilisateurs actuels et permettre une croissance à la longue. L'augmentation des exigences de sécurité pour certains fonctionnaires ne devrait pas réduire la capacité de SPC à réaliser des économies, dans la fourniture d'une solution plus économique, pour la plupart des fonctionnaires. SPC souhaite tenir des consultations avec l'industrie afin d'obtenir une réponse optimale au chapitre de la segmentation des utilisateurs, de l'information, de la sécurité des systèmes en général et des options de prestation.

4.1.4 Pressions liées à la protection des renseignements personnels

Les Canadiens sont très inquiets de la protection des renseignements personnels, surtout dans le contexte de la prestation de services électroniques. Le GC est déterminé à protéger la confidentialité des renseignements personnels utilisés dans le cadre des programmes et services au public, que ceux-ci soient offerts en personne, par courrier, par téléphone ou en ligne.

Les activités des ministères du GC reposent sur des politiques découlant de la *Loi sur la protection des renseignements personnels*[14], qui fixe le droit des Canadiens d'exercer un contrôle sur la collecte, l'utilisation et la communication de leurs renseignements personnels.

4.1.5 Prestation de services uniformes

Au gouvernement du Canada, il n'existe aucune norme unique sur les courriels. Les Canadiens et les entreprises sont souvent étonnés, et embêtés, par la complexité de la structure des systèmes de courriel de l'État et la diversité des conventions d'appellation appliquées par les ministères et organismes.

SPC prévoit mettre en œuvre une nouvelle solution de courriel qui :

(i) sera simple, efficace et utile pour les communications avec les citoyens et les entreprises;

[13] http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578
[14] http://laws-lois.justice.gc.ca/fra/lois/P-21/index.html

(ii) reposera sur une convention d'appellation unique et uniforme pour tous les employés du gouvernement du Canada, par exemple, jeanne.tremblay@canada.gc.ca[15].

À l'interne, l'ITSC permettra de résoudre des difficultés opérationnelles. Par exemple, elle :

(i) facilitera l'interopérabilité en améliorant les fonctions courriel et calendrier pour SPC et ses partenaires;

(ii) augmentera les fonctions de libre-service pour que les utilisateurs du courrier électronique puissent mieux gérer leurs boîtes de courriel, retrouver des courriels archivés, etc; et,

(iii) normalisera les niveaux de service pour garantir la prestation uniforme des services de courriels pour SPC et ses partenaires.

4.1.6 Souveraineté des données

Il incombe à SPC de protéger tous les référentiels et entrepôts de données utilisés par ses ministères et organismes partenaires. La protection de ces renseignements est, du point de vue de la confidentialité et de la sécurité, essentielle pour l'intégrité des programmes du gouvernement qui raffermit la confiance dans le GC.

De plus, l'ITSC doit impérativement respecter les exigences de confidentialité et de sécurité pour garantir la protection des renseignements personnels et confidentiels. Les Canadiens s'attendent à ce que le GC prenne toutes les mesures nécessaires pour protéger ces renseignements.

Surtout, les renseignements gérés par le fournisseur éventuel de la solution de courriel, y compris les courriels, les pièces jointes et les renseignements sur les utilisateurs des courriels, sont la propriété intellectuelle exclusive du GC et doivent être réputés comme relevant du GC, aux termes de la *Loi sur l'accès à l'information et toute autre législation.*

Les services et l'infrastructure de courriel de l'ITSC en seront établis au Canada. Des mesures contractuelles et techniques rigoureuses seront mises en place pour veiller à ce que les renseignements du gouvernement, qu'ils soient actifs ou inactifs, soient protégés en permanence ou consultés uniquement par des Canadiens autorisés à accéder à l'infrastructure de courriel, aux fins approuvées par l'ITSC.

Toute entente contractuelle future entre le Canada et un fournisseur éventuel de la solution de courriel doit donc tenir compte des points suivants :

(i) Droit du Canada d'ordonner la destruction ou la suppression des données

(ii) Conformité du fournisseur de solutions de courriel avec les instruments de politique et les pratiques du gouvernement du Canada en matière de

[15] La convention d'appellation indiquée ici n'est donnée qu'à titre d'exemple et n'a pas encore été finalisée par le Canada.

confidentialité et de sécurité, et notification du gouvernement du Canada concernant les atteintes à la confidentialité et à la sécurité

(iii) Preuve de formation et de sensibilisation en matière de confidentialité et de sécurité des employés du fournisseur de solutions de courriel qui auront accès aux éléments pertinents de la solution de courriel

4.2 Objectif opérationnel et avantages

L'objectif opérationnel de SPC mentionné dans le Rapport sur les plans et les priorités pour 2012-2013[16] est le suivant :

> Les services obligatoires sont fournis de façon regroupée et normalisée pour contribuer à l'exécution de programmes et à la prestation de services du gouvernement du Canada destinés à la population canadienne. [17]

L'ITSC permettra de regrouper et de moderniser les services de courriels gérés par SPC pour lui-même et ses partenaires afin de réduire les coûts, d'accroître la sécurité et d'améliorer l'exécution des programmes pour les citoyens canadiens et les entreprises. SPC offrira le nouveau service aux autres organismes du GC de manière facultative.

L'ITSC fournira les avantages suivants :

(i) Réduction des coûts opérationnels des services de courriels;;

(ii) Amélioration continue de la posture de sécurité des services de courriels afin que les programmes et les services puissent être offerts de manière sécuritaire et fiable à la population canadienne;

(iii) Amélioration de l'interopérabilité parmi les partenaires de SPC;

(iv) Normes d'appellation uniformes;

(v) Niveaux de service communs pour tous les utilisateurs;

(vi) Solution de courriel sécurisée et fiable pouvant traiter les courriels – Un système de niveau Secret (incluant renseignements de niveau Classifié jusqu'au niveau Secret et renseignements Protégés jusqu'au niveau Protégé C) et/ou un système Protégé jusqu'au et incluant le niveau Protégé B.

[16] http://www.tbs-sct.gc.ca/rpp/2012-2013/index-fra.asp?acr=2024

[17] Rapport sur les plans et les priorités de SPC, février 2012

5. APPROCHE D'APPROVISIONNEMENT PROPOSÉE

Dépendant de l'avis reçu lors des consultation de l'industrie, la stratégie d'approvisionnement pourrait inclure de multiples activités parallèles ou séquentielles. Pour les besoins complexes comme la transformation et la solution de l'ITSC, la solution d'approvisionnement collaboratif (SAC) est l'approche d'approvisionnement proposée. Une description de chaque étape de la SAC est fournie dans les sous-sections suivantes.

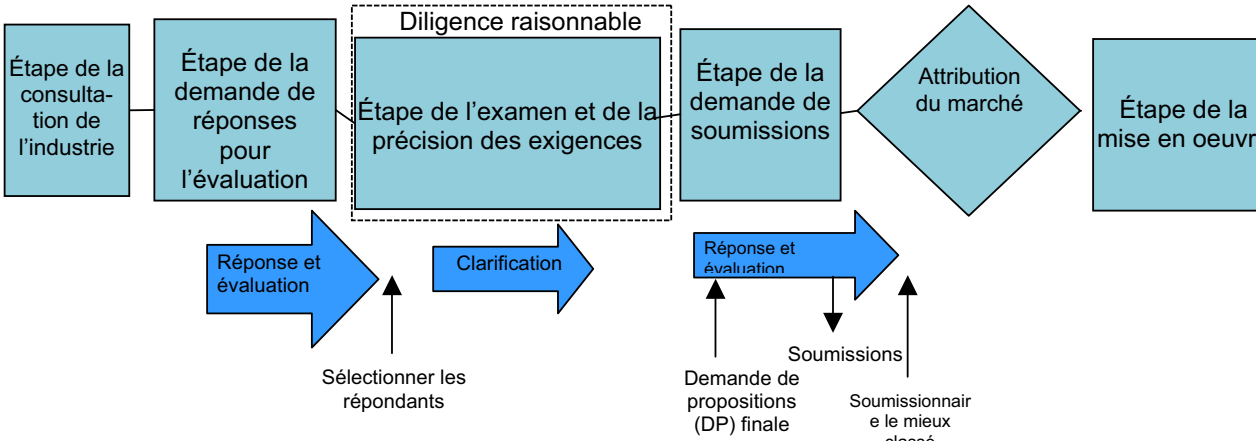
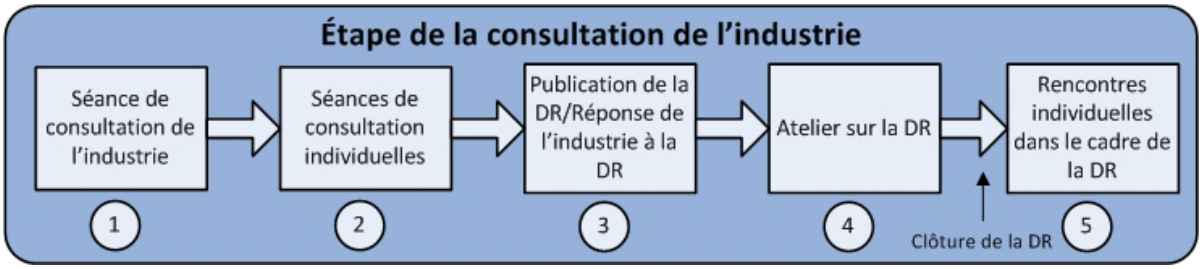


Figure 1 : SAC

5.1 Étape de la consultation de l'industrie

La première étape de la SAC est « l'étape de la consultation de l'industrie ». Au cours de cette étape, le Canada communiquera ses attentes aux organisations qui souhaitent fournir une solution de courriel au gouvernement du Canada. Cette étape vise à obtenir l'avis de l'industrie sur les exigences et l'approche en matière d'approvisionnement. Elle comprend cinq éléments principaux :



1. Assemblée de la Journée de l'industrie (terminée)
2. Séances de consultation individuelles de l'industrie (terminées)
3. demande de renseignements et ses réponses
4. Atelier sur la DDR destiné à l'industrie. Le Canada tiendra des séances d'une journée entière pour renseigner les répondants sur la situation actuelle des systèmes de courriel

de SPC ainsi que la portée de la nouvelle solution de courriel et les exigences et les difficultés techniques connexes. Les répondants pourront ainsi fournir dans leur réponse à la DDR des renseignements supplémentaires qui permettront au Canada de prendre des décisions plus éclairées dans le cadre de sa stratégie et de ses exigences de transformation des systèmes de courriel. Cette séance est prévue provisoirement pour le 5 juillet 2012 dans la région de la Capitale Nationale et le service de vidéoconférence sera disponible pour les régions. Un comité formé de plusieurs représentants du gouvernement du Canada présentera des renseignements et répondra aux questions de l'industrie. Le formulaire d'inscription et les renseignements logistiques pour ces séances sont fournis à l'annexe J. Veuillez envoyer le formulaire dûment rempli, par courriel, à l'attention de l'autorité contractante de TPSGC, indiquée à la section 2.8, au plus tard à 16 h (heure avancée de l'Est), le 27 juin 2012. Le Canada n'a pas l'intention de limiter le nombre de représentants pouvant assister aux séances par répondant, mais les répondants sont priés de mentionner le nombre approximatif de personnes de leur organisation qui y assisteront, afin que le Canada puisse déterminer un endroit/une salle où tenir les séances de l'atelier sur la DDR. Le Canada informera après coup les parties ayant envoyé le formulaire de l'annexe J de l'endroit/de la salle où auront lieu ces séances, au plus tard à 16 h (heure avancée de l'Est), le 3 juillet 2012.

5. Réunions individuelles possibles sur la demande de renseignements : Après clôture de la DDR, à la discrétion du Canada, des réunions pourront avoir lieu avec les répondants pour obtenir des précisions ou des explications supplémentaires sur leur réponse à la DDR.

5.2 Étape de la demande de réponses pour l'évaluation

Pendant cette étape, le Canada publiera une demande de réponses pour évaluation afin d'établir un sous-ensemble de répondants retenus possédant les compétences et l'expérience démontrées qui sont nécessaires pour mettre en œuvre et gérer la nouvelle solution de courriel regroupée. Les répondants retenus passeront alors à l'étape de l'examen et de la précision des exigences et seront invités à soumettre leur proposition en réponse à ces exigences, dans le cadre de l'étape de la demande de soumissions.

Les critères d'évaluation proposés de la demande de réponses pour l'évaluation porteront sur l'expérience du répondant et son aptitude à fournir des services de courriels de manière sécurisée et rapide en tenant compte des paramètres de taille, de portée et de complexité. De plus, la stabilité financière et la cote de sécurité sont des critères organisationnels importants. Les répondants doivent répondre à ces critères tout au long du processus. Le Canada peut, à sa seule discrétion, expulser les répondants du processus s'ils cessent de répondre à ces critères. De façon générale, la partie III contient les exigences obligatoires prévues, et l'annexe D renferme les critères d'évaluation proposés concernant l'étape de la demande de réponses pour l'évaluation. Le Canada peut envisager de reporter les points assignés à l'étape de la demande de réponses pour l'évaluation à l'évaluation finale de la DP.

5.3 Étape de l'examen et de la précision des exigences

Au cours de cette étape, les répondants retenus à l'étape précédente (c'est-à-dire à l'étape de la demande de réponses pour l'évaluation) collaboreront avec le Canada pour examiner et finaliser les exigences techniques ainsi que les exigences de la demande de soumissions, notamment :

(i) les exigences opérationnelles, fonctionnelles, architecturales, sécuritaires et techniques de la solution de courriel et de ses interfaces avec les applications de bureau et les applications opérationnelles;

(ii) les exigences de conversion des applications, comme les interfaces des programmes d'application standard;

(iii) les exigences de conversion des données, comme le stockage des courriels actifs, le stockage des courriels archivés et les interfaces de l'annuaire;

(iv) les exigences de planification de la transition, pour veiller à ce que SPC et ses partenaires puissent adopter la solution de courriel sans problème et sans interruption du service ni perte de données;

(v) les exigences d'évaluation de la sécurité et d'autorisation qui s'appliquent à la conception, à la mise en œuvre et à l'utilisation de la solution, conformément aux normes et aux lignes directrices du gouvernement;

(vi) les exigences de gestion des systèmes et du cycle de vie pour l'utilisation continue de la solution de courriel;

(vii) les modalités, l'évaluation, la structure de prix qui en découle, etc.

Pendant cette étape, les répondants retenus pourront être invités à démontrer comment leur solution permettra de répondre aux exigences définies. On pourra demander à chaque répondant retenu de créer, à ses propres frais, un environnement de validation de principe contenant jusqu'à 50 utilisateurs d'essai et accessible par Internet. Les données utilisées dans l'environnement de validation de principe seront des données d'essai non classifiées. Dans chaque environnement de validation de principe, le personnel de soutien des répondants retenus doit être en mesure de résoudre rapidement les problèmes cernés. L'environnement de validation de principe a plusieurs objets, notamment :

(i) examiner et vérifier les exigences de service de l'ITSC, et en discuter;

(ii) valider les risques et les hypothèses;

(iii) exécuter des essais sur la migration des données de Microsoft Exchange;

(iv) effectuer des essais sur la migration des données d'IBM Lotus Notes ou de Domino;

(v) procéder à des essais sur la migration des données de Novell GroupWise;

(vi) faire des essais sur l'intégration des applications avec des applications clés précises.

Le Canada utilisera les résultats de cette étape pour finaliser les exigences de la demande de propositions (DP) au cours de l'étape de la demande de soumissions, et non pour évaluer les répondants retenus ou les soumissionnaires.

5.4 Étape de la demande de soumissions

Pendant l'étape de la demande de soumissions, le Canada enverra la DP officielle aux répondants retenus qui auront franchi l'étape de l'examen et de la précision des exigences.

La DP leur permettra alors de répondre de manière officielle à l'ensemble des exigences. Le Canada peut envisager de reporter les points assignés à l'étape de la demande de réponses pour l'évaluation à l'évaluation finale de la DP. Le processus de report des points assignés à l'étape de la demande de réponses pour l'évaluation sera clairement défini dans la demande de réponses pour l'évaluation.

Dès qu'il recevra les propositions, le Canada procédera à une évaluation complète de chaque proposition et choisira celle qui offre le meilleur rapport qualité-prix aux Canadiens.

5.5 Étape de l'attribution du marché et de la mise en œuvre

Le Canada pense que la période de mise en œuvre et de migration pour la solution de courriel devrait durer de 18 à 24 mois pour SPC et ses partenaires, et le Canada s'attend à ce que la mise en œuvre de la nouvelle solution de courriel et la migration à celle-ci se termine d'ici mars 2015. Par ailleurs, le Canada envisage d'attribuer un marché de cinq ans et de trois périodes optionnelles d'un an. Cette période contractuelle comprend la période de mise en œuvre et de migration. Le Canada déterminera officiellement la durée du marché et les prolongations optionnelles à une étape ultérieure du processus d'approvisionnement.

5.6 Calendrier prévu de la SAC

Étape	Durée prévue
Consultation de l'industrie	De mai à juillet 2012
Demande de réponses pour l'évaluation	Août et septembre 2012
Examen et précision des exigences	D'octobre à décembre 2012
Demandes de soumissions	De janvier à mars 2013
Attribution du marché	Avril et mai 2013

6. PORTÉE

6.1 Portée de la transformation des services de courriels

6.1.1 Portée fonctionnelle

La portée fonctionnelle générale est définie ci-dessous. Les éléments précis de la portée et les exigences sous-jacentes (c'est-à-dire l'harmonisation avec la vision et la stratégie, l'utilisation des normes et l'intégration avec les services actuels de SPC) seront affinés et documentés de façon plus détaillée à l'étape de l'examen et de la précision des exigences.

L'annexe B, Matrice sur la portée de l'ITSC, contient un résumé plus complet de la portée actuelle de l'ITSC.

Inclus dans la portée

(i) Courriels
(ii) Messagerie instantanée
(iii) Calendrier
(iv) Contacts personnels
(v) Dossiers de courriels personnels et partagés
(vi) Intégration des services de courriels et de télécopies
(vii) Accès à un historique des courriels (archivage de courriels)
(viii) Courriel et annuaire
(ix) Antivirus et anti-pollupostage
(x) Gestion des appareils de télécommunication mobile (BlackBerry, téléphones intelligents, tablettes).

Non inclus dans la portée

(i) Corbeille arrivée intégrée (p. ex. intégration de messagerie vocale)
(ii) Espaces de travail favorisant la collaboration
(iii) Wikis, blogues et forums
(iv) Suites bureautiques (à l'exception des utilisateurs de courriel).

6.1.2 Autre portée

L'autre portée est définie ci-dessous. L'annexe B, Matrice sur la portée de l'ITSC, contient un résumé plus complet de la portée actuelle de l'ITSC.

- Inclus dans la portée

(i) Un système de niveau Secret (incluant renseignements de niveau Classifié jusqu'au niveau Secret et renseignements Protégés jusqu'au niveau Protégé C) et/ou un système Protégé jusqu'au et incluant le niveau Protégé B.

(ii) Tous les partenaires de SPC au Canada ainsi que les ambassades et les missions à l'étranger

(iii) Migration et transition des données

(iv) Soutien à la mise en œuvre et à la formation

(v) Soutien continu des courriels et des utilisateurs

(vi) Soutien à l'intégration des applications « ministérielles » et des applications de « programmes » du gouvernement du Canada (à l'aide de trousses d'outils d'interface normalisées)

Non inclus dans la portée

(i) Systèmes de courriel (niveau Très secret)

(ii) Services de courriels pour les plateformes physiques mobiles (comme les navires militaires du ministère de la Défense nationale)

(iii) Gestion du bureau (à l'exception des utilisateurs de courriel)

6.1.3 Interfaces des applications

L'initiative prévoit le remplacement des applications intégrées actuelles par des applications ministérielles et opérationnelles des ministères et des organismes partenaires.

Selon la stratégie actuelle, l'équipe de l'ITSC sera chargée d'établir un cadre de travail, un document d'orientation et une trousse d'outils pour l'intégration des systèmes de courriel. Les ministères et les organismes seront chargés de modifier leurs applications afin de les intégrer à la nouvelle solution de courriel.

6.2 Résumé de l'état actuel des systèmes de courriel

L'annexe C, Sommaire de l'état actuel, contient un résumé sur les systèmes de courriel actuels des partenaires de SPC, ainsi que des données volumétriques prévues.

6.3 Exigences obligatoires

La partie III, Exigences obligatoires prévues, contient un aperçu de certaines exigences obligatoires prévues que le Canada considère comme importantes pour l'étape de la demande de soumissions.

7. OPTIONS CONCERNANT LA PRESTATION DE SERVICES DE COURRIELS

Le Canada a envisagé un certain nombre d'options de prestation de services pour la gestion et la mise en œuvre d'une solution de courriel. Avant de prendre des décisions définitives sur la prestation de services, il a besoin de plus d'informations de la part de l'industrie sur deux des options : les services gérés et l'impartition. Ces options sont définies ci-après.

SPC souhaite obtenir l'avis de l'industrie sur ces deux options ou sur une option de prestation de services qui, selon elle, devrait être envisagée par SPC comme l'option de prestation des services de courriels la plus viable et la plus rentable pour le gouvernement du Canada. Des décisions finales sur la stratégie de prestation des services seront prises au cours des phases subséquentes du projet.

Il convient aussi de noter que le Canada a énormément investi dans le matériel, les logiciels, la formation et l'intégration des applications dans les solutions de courriel actuelles. SPC a l'intention de mettre ces investissements à la disposition de l'industrie en tant qu'équipement fourni par le gouvernement (EFG). SPC souhaite savoir si l'industrie compte tirer profit de cet investissement pour fournir le meilleur rapport qualité-prix au Canada et comment elle le ferait. Plus précisément, il souhaite savoir quelles sont les recommandations de l'industrie sur la façon dont le Canada doit évaluer les propositions futures selon un coût total de possession comprenant tous les coûts liés à la migration, à l'intégration et à la formation. Il convient de noter qu'en ce moment, le Canada n'a pris aucune décision sur la manière dont seront exploités les investissements actuels dans l'équipement fourni par le gouvernement (matériel et logiciels). Le Canada cherche à obtenir l'avis de l'industrie sur des solutions possibles.

7.1 Description de l'option du service géré

Un fournisseur de solutions de courriel du secteur privé travaillant dans un centre de données géré par SPC serait responsable de la création et de la mise en service de la nouvelle solution de courriel. Une fois la nouvelle solution créée, SPC et ses partenaires passeraient à celle-ci avec l'aide d'un fournisseur de solutions de courriel du secteur privé. La solution serait dirigée et gérée par un fournisseur de solutions de courriel du secteur privé.

Pour cette option de prestation de services, le Canada est ouvert à un éventail de scénarios concernant la propriété des actifs, le soutien des applications et des interfaces et la fourniture de l'infrastructure de centre de données et de sécurité. Les services de connectivité réseau visant les dispositifs pour utilisateurs finaux seront fournis par SPC.

7.2 Description de l'option du service imparti

SPC impartirait le service de courriel à un fournisseur de solutions de courriel du secteur privé possédant les ressources matérielles et logicielles ainsi que serait responsable de la prestation de tous les services professionnels nécessaires pour fournir le service de courriel. Le Canada conclurait un marché pour que le fournisseur de solutions de courriel planifie, crée et gère la solution de courriel proposée. Le service serait fourni dans des centres de données situés au Canada et gérés par le fournisseur de solutions de courriel. Les services de connectivité réseau visant les dispositifs pour utilisateurs finaux seront fournis par SPC.

La partie IV contient des questions précises liées à ces deux options.

8. GESTION DES RISQUES LIÉS À LA SÉCURITÉ DE LA TI

Dans un monde où la menace évolue sans cesse, compte tenu des contraintes financières du gouvernement du Canada, la sécurité de la TI ne peut plus passer au second plan. Elle doit être un élément essentiel de tous les grands projets. La sécurité est donc une des pierres angulaires des étapes de lancement et de planification de l'ITSC.

Le Centre de la sécurité des télécommunications Canada (CSTC) rédige un document sur l'approche du cycle de vie intitulé « Lignes directrices en matière de sécurité des technologies de l'information (ITSG-33) », dans lequel il recommande des processus permettant aux ministères et organismes fédéraux de veiller à ce qu'on tienne compte de la sécurité dès le début de la mise en œuvre de leur système de TI et à ce que leurs systèmes et leurs organisations s'améliorent constamment afin d'évoluer au même rythme que les menaces pesant sur l'environnement de TI.

Le document ITSG-33 contient un catalogue des contrôles de sécurité structurés en trois catégories : les contrôles techniques, les contrôles opérationnels et les contrôles de gestion. Ces trois catégories de contrôle de sécurité représentent un groupe d'exigences de sécurité normalisées couvrant tous les aspects des systèmes et des organisations.

Une version provisoire des contrôles de sécurité disponibles est annexée à la présente DDR et doit être téléchargée par les répondants, comme l'indique la pièce jointe n^{o} 2 de la présente DDR. Veuillez prendre note que la version du document ITSG-33 est provisoire et que ce texte peut être modifié par le CSTC. Le Canada contextualisera et sélectionnera les contrôles de sécurité nécessaires pendant l'étape de planification afin d'établir une base de référence des exigences de sécurité qui tiendra bien compte des menaces et des vulnérabilités évaluées et réduira les risques de sécurité pour SPC et ses partenaires.

PARTIE III : EXIGENCES OBLIGATOIRES PRÉVUES

9. EXIGENCES OPÉRATIONNELLES ET FONCTIONNELLES

9.1 Service regroupé de courriel

La solution de courriel doit regrouper et moderniser les services de courriels obligatoires de SPC que ce dernier gère pour lui-même et ses partenaires à l'intérieur de la période contractuelle précisée à la partie II – Données fondamentales sur l'ITSC - section 5.5. Une fois la mise en œuvre et la migration terminées pour SPC et ses partenaires, la solution de courriel doit être mise à la disposition d'autres organismes du GC avec les mêmes services et niveaux de service. Les autres organismes du GC peuvent décider d'adopter cette solution de courriel si SPC estime que cela est possible. Il n'y a aucun engagement quand au nombre de boîtes aux lettres ou au moment de l'activation de la solution de courriel pour le reste des organismes du GC.

9.2 Convivialité

Le nouveau système de courriel doit être convivial et intuitif et n'exiger aucune formation officielle. Une formation à l'aide de documents ou de tutoriels en ligne de moins de 60 minutes serait considérée comme le maximum.

9.3 Accessibilité

La solution de courriel doit être mise à la disposition de tous les partenaires de SPC, où qu'ils se situent au Canada, et de toutes les ambassades et missions à l'étranger, grâce à un accès par l'infrastructure du réseau du GC. La solution de courriel doit être disponible dans les deux langues officielles et permettre aux utilisateurs de changer de langue de façon dynamique sans faire appel à un administrateur. La solution de courriel doit répondre aux normes d'accessibilité, d'après la Norme d'accès facile du SCT[18], et être adaptée aux personnes qui ont des besoins particuliers (p. ex. elle doit être interopérable avec les applications destinées aux employés qui ont une déficience visuelle ou auditive).

9.4 Aide à la mobilité

La solution de courriel doit supporter des fonctions de gestion des appareils mobiles pour des plateformes comme les téléphones intelligents BlackBerry[MD] de Research in Motion, les téléphones intelligents iPhone[MD] et les iPad[MD] d'Apple, les tablettes ainsi que les téléphones intelligents et les tablettes Android[MC]/Windows[MD].

9.5 Disponibilité et fiabilité

La cible relative au temps de disponibilité de la solution de courriel, pour les utilisateurs, est de 100 %, 24 h sur 24, 7 jours sur 7 et 365 jours par année.

9.6 Recherche élargie intelligente

La solution de courriel doit permettre à l'utilisateur final de rechercher des messages électroniques et du contenu.

[18] http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12044&section=text

9.7 Soutien administratif local des courriels

La solution de courriel doit permettre au personnel de SPC et de ses partenaires de remplir des fonctions d'administration des courriels, notamment l'ajout ou la suppression de comptes et la réinitialisation de mots de passe.

9.8 Respect des lois et des politiques

La solution de courriel doit respecter les lois actuelles et les instruments du Secrétariat du Conseil du Trésor (SCT), comme les politiques, les normes et les lignes directrices. Nota : Le SCT se penche actuellement sur les lacunes relatives aux politiques que peut entraîner la mise en œuvre d'un service de courriel « intergouvernemental ». Veuillez consulter l'annexe G, Instruments législatifs et instruments de politique du Secrétariat du Conseil du Trésor pour obtenir une première liste des instruments pouvant influer sur ce projet. Cette liste peut être modifiée.

9.9 Respect des délais

La date de fin prévue pour la mise en œuvre et la migration est le 31 mars 2015 pour SPC et ses partenaires.

9.10 Rentabilité

Cette initiative doit permettre au gouvernement du Canada de fournir des services de courriels à un coût comparable à celui de l'industrie.

10. EXIGENCES DE LA PLATEFORME TECHNOLOGIQUE

10.1 Soutien « normes ouvertes »

La solution de courriel doit être conforme aux normes de l'industrie et utiliser des interfaces normalisées ouvertes et non exclusives. L'annexe B, Matrice sur la portée de l'ITSC contient des exemples d'interfaces.

10.2 Trousse à outils d'intégration des systèmes en place

La solution de courriel doit prévoir une trousse à outils d'intégration que SPC et ses partenaires pourront utiliser pour intégrer leurs applications à la nouvelle solution de courriel.

10.3 Gestion de l'accès

La solution de courriel doit permettre de gérer les profils d'utilisateur, les attestations ainsi que le processus d'authentification et d'autorisation.

11. EXIGENCES DE MISE EN ŒUVRE ET DE MIGRATION DES DONNÉES

11.1 Migration des courriels

Le contenu et les données des courriels existants, y compris les pièces jointes, doivent être transférés dans le nouveau système.

L'entrepreneur doit :

a) offrir des solutions de formation et de migration des données qui permettront au Canada de réduire le coût, la complexité et les risques dans le cadre de la transition;

b) fournir aux ministères et aux organismes des outils d'intégration des applications et des interfaces conformes aux normes de l'industrie, comme l'indique l'annexe B – Matrice sur la portée de l'ITSC, pour faciliter l'intégration de la solution de courriel à leurs applications existantes;

c) communiquer aux ministères et aux organismes des directives qui réduiront au minimum l'effort de transition, l'effet sur les opérations et le risque de perte de données et de rendement de la messagerie électronique dans le cadre de l'intégration de la solution de courriel à leurs applications existantes;

d) assumer le coût de la formation et de la migration, estimé par le fournisseur et validé et convenu par SPC, lié à la transition vers une nouvelle technologie de messagerie, si elle diffère des plateformes de courriel existantes utilisées par SPC et ses partenaires.

L'entrepreneur ne sera tenu de fournir que les interfaces normalisées et ne sera pas responsable de l'intégration des applications actuelles à la solution de courriel.

11.2 Transition sans heurts

Les fonctions existantes doivent être en place durant la transition pour permettre aux utilisateurs de conserver un accès aux services de courriels, en tout temps, pendant la transition.

12. EXIGENCES DE GESTION DES SERVICES DE TECHNOLOGIE DE L'INFORMATION

12.1 Intégration de la gestion des services de technologie de l'information

L'entrepreneur devra intégrer les processus et les outils de gestion des services de technologie de l'information (ITSM) de SPC et de ses partenaires. Veuillez prendre note que le niveau d'intégration devrait varier selon l'option de prestation de services de courriels retenue.

13 EXIGENCES EN MATIÈRE DE SÉCURITÉ

13.1 Niveaux de sécurité multiples

Le nouveau service de courriel sera certifié pour gérer des courriels: un système de niveau Secret (incluant renseignements de niveau Classifié jusqu'au niveau Secret et renseignements Protégés jusqu'au niveau Protégé C) et/ou un système Protégé jusqu'au et incluant le niveau Protégé B.

13.2 Sécurité multi-niveaux

Le service doit appuyer des contrôles de sécurité multi-niveaux, comme :

- des services de sécurité du périmètre (p. ex. pare-feu, contrôles antivirus et contrôles anti-pollupostage);
- la protection des menaces issues des données inactives (p. ex. contrôle de l'accès);
- la protection des données actives (p. ex. cryptage).

13.3 Soutien de l'infrastructure à clés publiques

La solution de courriel doit appuyer des extensions S/MIME. Le GC modifie ses exigences relatives au soutien de l'infrastructure à clés publiques, et la solution de courriel devrait supporter ces nouvelles normes à mesure qu'elles seront élaborées.

13.4 Citoyenneté canadienne pour le personnel de soutien

Tous les employés du soutien technique et d'ingénierie doivent être des citoyens canadiens.

13.5 Souveraineté des données

Toutes les composantes de l'infrastructure de données du système de courriel doivent être hébergées au Canada.

a) Tous les serveurs de courriel et tous les dépôts de données doivent être hébergés au Canada.

b) Les entrepôts d'objets média utilisés pour la sauvegarde, la récupération des données, l'archivage historique ou à d'autres fins doivent être hébergés dans des endroits sécurisés et approuvés au Canada.

c) La solution de courriel doit permettre de contrôler ou de surveiller l'accès aux dépôts de données et à d'autres systèmes informatiques, de manière que le Canada puisse, à sa discrétion, surveiller, vérifier ou restreindre l'accès aux données du Canada. Ces activités doivent comprendre un mécanisme de journalisation et de signalement permettant d'identifier toutes les personnes qui ont accédé aux composantes du système de courriel à des fins d'utilisation et de maintenance.

d) Tous les courriels internes du gouvernement du Canada envoyés par des utilisateurs du gouvernement situés au Canada ou à l'étranger à d'autres utilisateurs du gouvernement situés au Canada ou à l'étranger doivent passer par des réseaux protégés adéquats. Les courriels transférés par des fournisseurs qui ne répondent pas expressément à ces deux conditions ne seront pas acceptés. Les données en transit ne

doivent pas être sauvegardées/stockées de leur point de départ à leur point d'arrivée; et,

e) En cas d'accès non autorisé aux données du Canada (c'est-à-dire si cet accès n'a pas été autorisé de manière officielle par le Canada) dans la solution de courriel (p. ex. pour respecter une ordonnance de communication d'un État étranger), la responsabilité du fournisseur de solutions de courriel vis-à-vis du Canada pour cet accès autorisé ne sera pas limitée.

13.6 Menaces relatives à l'approvisionnement pour le gouvernement du Canada

Outre la menace de cyberattaques, on est de plus en plus conscient des risques posés par les technologies potentiellement vulnérables ou modifiées qui pourraient pénétrer dans les réseaux de communication et l'infrastructure de TI du gouvernement du Canada par l'intermédiaire de menaces à l'approvisionnement.

L'entrepreneur doit transmettre au gouvernement du Canada une liste contenant les noms de tous les fabricants et fournisseurs de matériel et de logiciels qu'il propose d'utiliser pour l'infrastructure et les services de TI de l'ITSC avant de conclure un marché avec eux. Le Canada se réserve le droit de rejeter un fabricant ou un fournisseur de matériel ou de logiciels pour des motifs de sécurité ou de stabilité opérationnelle.

L'entrepreneur doit respecter les Lignes directrices sur la chaîne d'approvisionnement des technologies (LDCAT) :

Français :
HTML : http://www.cse-cst.gc.ca/its-sti/services/tscg-ccat/tscg-ccat01g-fra.html

PDF: http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01g-fra.pdf

http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01l-fra.pdf

Anglais :

HTML : http://www.cse-cst.gc.ca/its-sti/services/tscg-ccat/tscg-ccat01g-eng.html

PDF : http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01g-eng.pdf

http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01l-eng.pdf

Dans le cadre de la Journée de l'industrie qui a eu lieu le 12 juin 2012, le Centre de la sécurité des télécommunications du Canada (CSTC) a présenté aux entreprises sur place des renseignements non classifiés sur la cybersécurité et sur les menaces à l'approvisionnement.

Le CSTC a offert de fournir aux organisations intéressées à participer aux étapes subséquentes du processus d'approvisionnement lié à l'Initiative de transformation des services de courriels des renseignements délicats sur les menaces à l'approvisionnement. Une ou deux séances d'information seront offertes de juin à juillet 2012, à l'étape de la consultation de l'industrie (voir la

section 5,6). Les organisations devront s'inscrire directement auprès de TPSGC. Au moins une des personnes présentes à la séance devrait avoir des pouvoirs décisionnels en matière de sécurité, de technologie ou d'approvisionnement (p. ex. VP/DPT, ASE, etc.). Tous les représentants des organisations qui comptent participer aux séances d'information sur les menaces à l'approvisionnement doivent signer l'entente de confidentialité qui se trouve à l'Annexe H et l'envoyer avec leur formulaire d'inscription (décrit ci-dessous et disponible à l'annexe I). Cette entente n'est pas négociable et doit être signée par un dirigeant de l'entreprise qui a les pouvoirs nécessaires pour accepter les modalités de l'entente. Une fois signée, l'entente de non-divulgation doit être envoyée par courriel à l'autorité contractante de TPSGC dont les coordonnées apparaissent à la section 2,8 au plus tard le 27 juin 2012, à 16 h HAE. Moyennant l'approbation de l'entente par TPSGC et par le CSTC, les organisations seront ensuite conviées par TPSGC à une séance d'information sur les menaces à l'approvisionnement où ils recevront des renseignements de nature délicate.

Le Canada pourra, à sa discrétion, inviter des organisations individuelles ou des groupes d'organisations à assister aux séances d'information. Veuillez remplir le formulaire qui se trouve à l'annexe I et l'envoyer courriel à l'autorité contractante de TPSGC dont les coordonnées apparaissent à la section 2,8 au plus tard le 27 juin 2012, à 16 h HAE, afin d'aider TPSGC à coordonner la tenue des séances d'information. Le Canada déterminera quand les séances auront lieu et fournira des renseignements à cet effet à toutes les parties qui ont envoyé le formulaire de l'annexe I par courriel.

13.7 Attestation de sécurité

Une attestation de sécurité est une certification délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC). Les exigences liées à la sécurité seront établies dans la demande de réponses pour l'évaluation et dans la demande de propositions.

Le Canada prévoit que les répondants retenus et les soumissionnaires devront posséder les documents suivants :

a) **Cote de sécurité** du Canada pour les répondants retenus et les soumissionnaires qui devront consulter des renseignements de nature délicate.

b) **Attestation de sécurité d'installation (ASI) et Autorisation de détenir des renseignements (ADR)** de la Direction de la sécurité industrielle canadienne (DSIC) pour les installations où le répondant retenu ou le soumissionnaire souhaite utiliser et stocker les renseignements de nature délicate.

c) Capacité en matière de **sécurité des technologies de l'information** (CSTI) contrôlée par la DSIC pour les installations dans lesquelles le répondant retenu ou le soumissionnaire souhaite utiliser et stocker les renseignements de nature délicate,

afin que ce dernier puisse traiter, stocker ou transmettre des renseignements de nature délicate par voie électronique.

Les entreprises doivent s'attendre à ce que le personnel qui entre en fonction après l'étape de consultation de l'industrie doive obtenir une cote de sécurité de niveau Secret. Il convient de noter qu'à l'étape de la demande de propositions, tous les soumissionnaires doivent répondre à l'ensemble des exigences liées à la sécurité. Veuillez consulter l'annexe F - Liste de vérification des exigences relatives à la sécurité (LVERS) (version préliminaire).

Les répondants sont informés que les travaux et les services à fournir pour l'ITSC doivent comprendre des mesures de sécurité spéciales et être visés par des contraintes liées à la sécurité nationale. Les répondants retenus et les soumissionnaires doivent donc accepter les conditions établies dans la demande de réponses pour l'évaluation et dans la demande de propositions qui ont trait à la sécurité nationale et à l'intérêt national et qui nécessitent une vérification et un contrôle des personnes désignées qui participent à l'ITSC. Les répondants doivent s'attendre à des exigences strictes et à la nécessité absolue de les respecter, y compris des exigences qui ont trait au traitement des renseignements de niveau Secret.

Le Ministère pense qu'il devra imposer une partie ou la totalité des obligations contractuelles et restrictions suivantes dans le cadre des contrats liés à l'ITSC :

a) Les employés de l'entrepreneur qui devront utiliser les schémas ou les documents de l'ITSC ou se rendre dans certains locaux du gouvernement et devront posséder une cote de sécurité de niveau Secret.

b) Toutes les personnes qui accompliront les tâches de l'entrepreneur dans le cadre de l'ITSC devront posséder une cote de sécurité du niveau adéquat. En conséquence, l'entrepreneur doit veiller à ce que les employés compétents aient une cote de sécurité du niveau exigé et à ce que ces cotes de sécurité soient traitées à l'avance afin qu'elles soient en leur possession, au besoin.

c) En ce qui a trait à l'option d'approvisionnement de services gérés, les employés détenant une cote de sécurité valide devront uniquement se rendre sur les lieux de travail indiqués et ne seront pas autorisés à pénétrer dans les zones d'accès limité.

d) En ce qui a trait à l'option d'approvisionnement de services gérés, les employés de l'entrepreneur ne pourront pas se rendre dans certains locaux s'ils ne sont pas accompagnés par le personnel autorisé ou s'ils ne possèdent pas la cote de sécurité exigée.

e) En ce qui a trait à l'option d'approvisionnement de services gérés, le Canada se réserve le droit d'établir les exigences des enquêtes de sécurité pour les employés de l'entrepreneur qui doivent se rendre dans les locaux pendant toute la durée du marché de l'ITSC.

f) En ce qui a trait à l'option d'approvisionnement de services gérés, les employés de l'entrepreneur qui doivent se rendre régulièrement dans certains locaux devront posséder une cote de sécurité de niveau Secret. Les employés qui ne travaillent pas dans les locaux à temps plein et auxquels l'entrepreneur a demandé d'accomplir certaines tâches au besoin devront être accompagnés par des employés autorisés, ou obtenir tout d'abord une cote de sécurité d'un niveau désigné, et,

g) Des exigences et des protocoles de sécurité seront en place pour veiller à ce que personne n'accède aux renseignements de nature délicate ou aux renseignements exclusifs gérés par l'entrepreneur, les installations et l'ITSC, sans avoir une cote de sécurité adéquate à la suite d'une affectation, d'une mutation ou d'une décision de l'entrepreneur, d'un changement de contrôle de l'entrepreneur, d'une procédure de recours de la part de prêteurs, ou d'un autre événement.

13.8 Processus de sécurité de la Direction de la sécurité industrielle canadienne

Les attestations de sécurité (octroyées par la DSIC) permettront au répondant de travailler dans les locaux du GC et d'avoir accès à des renseignements confidentiels ou délicats, au besoin. La Politique du gouvernement sur la sécurité prévoit que le personnel doit se soumettre à un filtrage de sécurité lorsque les fonctions ou les attributions demandent d'avoir accès à des renseignements ou à des biens protégés ou classifiés. Les répondants doivent être parrainés par un représentant de SPC pour enclencher le processus et obtenir une attestation de sécurité ou en obtenir une de niveau supérieur directement à l'appui de la l'ITSC. Ils peuvent envoyer leurs demandes à cet effet à la personne suivante :

Claude Bazinet

Coordonnateur de projet

Services partagés Canada

Regroupement des services de courriels

255, rue Albert, salle 1201-19

Ottawa (Ontario) K1P 6A9

Canada

Courriel : claude.bazinet@ssc-spc.gc.ca

Téléphone : 613-960-9253

Télécopieur : 613-941-2783

Nous invitons les soumissionnaires à présenter rapidement leurs demandes de cote de sécurité. Nous invitons de nouveau instamment les répondants à demander une cote de sécurité pour l'ensemble des principaux employés et toutes les autres personnes qui devront peut-être, pendant l'étape de l'examen et de la précision des exigences, consulter des renseignements de nature délicate ou accéder à des lieux sécurisés. Le processus d'attribution de marché ne sera pas retardé pour permettre aux fournisseurs d'obtenir les autorisations de sécurité nécessaires.

13.9 Protection des renseignements personnels

La solution de courriel doit garantir que seules les personnes autorisées auront accès aux renseignements, et doit respecter les obligations statutaires de la *Loi sur la protection des renseignements personnels*[19] et de la *Loi sur l'accès à l'information*[20].

[19] http://laws-lois.justice.gc.ca/fra/lois/P-21/index.html

[20] http://laws-lois.justice.gc.ca/fra/lois/A-1/index.html

PARTIE IV : QUESTIONS

14. QUESTIONS

Nous demandons aux membres de l'industrie de répondre aux questions ci-dessous, présentées par catégorie, et de formuler des commentaires à leur sujet que le Canada prendra en considération pour la mise en œuvre de l'ITSC. Veuillez justifier vos réponses pour permettre au Canada d'avoir plus d'information sur laquelle se fonder pour aller de l'avant.

N'hésitez pas à commenter tout aspect de la présente demande de renseignements ni à formuler des commentaires ou des recommandations générales concernant l'initiative.

Les questions qui suivent ont été regroupées en dix thèmes généraux. Les détails relatifs à chacun de ces thèmes seront présentés et feront l'objet de discussions au cours des ateliers tenus dans le cadre du processus de demande de renseignements. Les répondants doivent répondre à ces questions selon le contexte du matériel fourni.

1. Options concernant la prestation de services de courriels;
2. Exigences liées aux opérations, aux politiques, à la gestion de l'information et au fonctionnement;
3. Exigences de sécurité;
4. Exigences relatives à la protection des renseignements personnels;
5. Considérations liées à la plateforme technologique;
6. Mise en œuvre et migration;
7. Gestion des services et opérations;
8. Considérations socioéconomiques liées aux petites et moyennes entreprises;
9. Considérations liées à l'écologisation; et,
10. Approche proposée en matière d'approvisionnement.

14.1. Options concernant la prestation de services de courriels

La section 7 de la partie II – Données fondamentales sur l'ITSC - présente deux options de prestation de services pour l'approvisionnement en produits et services de courriels. Le Canada cherche à obtenir les commentaires des membres de l'industrie sur la viabilité des perspectives pour ces options de prestation de services.

Pour le moment, le Canada comprend bien les exigences liées aux technologies de messagerie électronique (fonctions des produits, infrastructure de serveurs et de stockage, composantes de client lourd et léger). Cependant, toute information supplémentaire sur ces technologies, plus particulièrement sur les idées novatrices dans ces secteurs, ajouterait aux connaissances du Canada dans le domaine.

Par-dessus tout, le Canada cherche à mieux comprendre les services et les occasions d'affaires offerts par les organisations du secteur privé en ce qui a trait à la conception, à la conversion, à la transition et aux exigences de gestion continue du système pour un service de courriel.

Q01 : **:** Pouvez fournir des études de cas et/ou une justification opérationnelle qui pourraient aider SPC dans son processus décisionnel visant à déterminer le meilleur modèle de prestation de services pour la mise en œuvre de la solution de courriel du GC?

Q02 :

(i) Avez-vous une préférence quant au modèle de prestation de services à adopter pour la solution destinée à SPC et à ses partenaires dans le cadre de l'Initiative de transformation des services de courriels et conformément au calendrier du projet pour l'envoi et la réception de courriels protégés (jusqu'au niveau Protégé B)? (Veuillez indiquer l'option de prestation de services décrite à la section 7 de la partie II) :

a) Service géré;

b) Service imparti;

c) Toute autre option dont le GC devrait tenir compte.

(ii)Le modèle que vous privilégiez changerait-il pour le traitement de courriels classifiés jusqu'au niveau Secret (y compris de niveau protégé C)? Le cas échéant, veuillez indiquer comment. Veuillez justifier votre réponse en indiquant au moins les avantages et les inconvénients des options dont le GC devrait tenir compte.

(iii) Cette recommandation changerait-elle si SPC séparait les exigences pour la prestation d'une solution pour le système des courriels Secret (incluant renseignements de niveau Classifié jusqu'au niveau Secret et renseignements Protégés jusqu'au niveau Protégé C) et/ou un système Protégé jusqu'au et incluant le niveau Protégé B. de niveau protégé (jusqu'au niveau Protégé B)?

Q03 : Êtes-vous en mesure de fournir à SPC et à ses partenaires une solution de courriel respectant le cadre de projet de l'ITSC pour des courriels protégés jusqu'au niveau Protégé B? Pouvez-vous le faire pour des courriels classifiés jusqu'au niveau Secret (y compris les renseignements de niveau Protégé C)? Veuillez justifier votre réponse.

Q04 : De quelle façon votre offre de services serait-elle touchée si le Canada acceptait uniquement une solution de courriel provenant d'une entreprise canadienne ou d'une filiale canadienne étrangère (une entreprise canadienne, exerçant ses activités au Canada, qui est une filiale d'une société mère étrangère) tout en respectant les exigences de l'ITSC et s'il limitait de plus le recours à des sous-traitants aux entreprises canadiennes et aux filiales canadiennes étrangères?

Q05 : Selon vous, quels sont les principaux risques de ce genre de projet de regroupement des services de courriels, et quelles mesures le Canada devrait-il prendre pour les atténuer. Veuillez indiquer les risques du point de vue de la planification, de la migration, de la mise en œuvre et du soutien.

14.2 Exigences liées aux opérations, aux politiques, à la gestion de l'information et au fonctionnement

SPC veut avoir l'opinion des membres de l'industrie sur la capacité des soumissionnaires à satisfaire aux exigences obligatoires prévues à la partie III.

Q06 : Existe-t-il des exigences de la partie III – Exigences obligatoires prévues ou Catalogue des contrôles de sécurité ITSB-33 - que votre organisation juge préoccupantes pour la mise en œuvre globale de la solution de courriel? Veuillez indiquer tout commentaire sur la complexité, le coût et les risques d'exécution liés aux objectifs, aux exigences opérationnelles, aux hypothèses et au modèle conceptuel de l'ITSC.

14.3 Exigences relatives à la sécurité

SPS a des exigences pour un système de niveau Secret (incluant renseignements de niveau Classifié jusqu'au niveau Secret et renseignements Protégés jusqu'au niveau Protégé C) et/ou un système Protégé jusqu'au et incluant le niveau Protégé B. Pour l'instant, le Canada n'a pas déterminé si une solution ou un fournisseur de services unique pourra répondre à ce besoin. Pour faciliter la prise de cette décision importante, SPC veut en savoir plus sur les capacités et l'expérience des membres de l'industrie quant à la fourniture et au soutien d'un système de courriel Secret. La section qui suit comprend donc des questions détaillées sur la protection des renseignements personnels. Les réponses à ces questions seront très utiles pour déterminer la stratégie de prestation de services à adopter

Q07 : Décrivez votre méthode actuelle de gestion des risques. Veuillez fournir les éléments suivants dans votre réponse :

a) Structure de gouvernance de la sécurité de votre organisation;

b) Processus de catégorisation des biens;

c) Processus d'évaluation de la menace et du risque;

d) Processus de surveillance et d'amélioration continues.

Q08 : Décrivez votre processus actuel d'ingénierie de la sécurité des systèmes d'information (p. ex. cycle de vie de la fourniture d'un système sécurisé). Veuillez fournir les éléments suivants dans votre réponse :

a) Structure de gouvernance du projet;

b) Activités de sécurité et livrables clés du processus;

c) Façon dont la sécurité serait intégrée à la coordination des décisions de développement, de mise en œuvre et de conception du système avec le GC tout au long du marché;

d) Méthodologie de codage sécurisé (le cas échéant).

Q09 : Décrivez votre architecture de sécurité conceptuelle (générale) pour la solution regroupée de courriel du GC. Si cela est possible, incluez les éléments ci-dessous dans votre réponse

a) Façon dont cette architecture conceptuelle tient compte des menaces énoncées au point 4.1.3 de la partie II- Donnée fondamentales sur l'ITSC;

b) Approche de gestion de l'identité et des comptes;

c) Approche de contrôle d'accès, y compris l'authentification des utilisateurs et des courriels, l'autorisation, les clients distants et la classification des courriels;

d) Chiffrement, y compris tout recours aux technologies de l'Infrastructure à clés publiques (ICP);

e) Approche pour assurer l'intégrité des courriels, y compris toute utilisation de la signature numérique;

f) Approche de protection des frontières;

g) Capacité des logiciels de marquage pour la classification de documents et de courriels;

h) Toute autre approche d'étiquetage de sécurité ou de droits de gestion, y compris le traitement sécuritaire de l'information inactive et en transit et l'intégration au contrôle d'accès;

i) Approche pour la sécurité Web;

j) Approche de protection par déni de service;

k) Approche de protection avec un système de noms de domaine (DNS);

l) Approche de protection contre les programmes malveillants (pièces jointes aux courriels);

n) Approche proposée pour protéger le GC contre les problèmes causés par des utilisateurs qui ouvrent des courriels avec des agents de menace intégrés, par exemple, une protection contre les virus, les vers et les pourriels.

Q10 : Décrivez vos processus opérationnels proposés pour la solution regroupée de courriel du GC. Veuillez fournir les éléments suivants dans votre réponse :

a) Approche de vérification, y compris la journalisation, la surveillance, le système de prévention des intrusions (SPI), le système de détection des intrusions (SDI) la gestion des incidents et l'approche d'intervention;

b) Approche pour la configuration sécuritaire et la gestion des changements;

c) Approches pour la migration sécuritaire du contenu des courriels existants et archivés à partir des anciens systèmes (p. ex. détection et destruction de logiciels malveillants);

d) Approche de protection pour l'accès aux supports, le stockage, le transport et le nettoyage;

e) Sauvegarde, redondance et mesures de protection d'urgence;

f) Approche de protection physique et environnementale;

g) Approche pour la sécurité du personnel;

h) Approche de protection des menaces à l'approvisionnement;

i) Toute norme utilisée pour les éléments ci-dessus.

Q11 : Décrivez votre capacité à respecter les exigences de surveillance et de vérification d'un tiers (GC). Veuillez fournir les éléments suivants dans votre réponse :

a) Échange de l'information liée aux vérifications de sécurité, y compris :

(i) les copies de toutes les transactions de messages non modifiées;

(ii) l'échange et la réception d'information sur les menaces;

b) Évaluation par un vérificateur externe de votre infrastructure de TI et de vos processus opérationnels (p. ex. examen du document de procédures opérationnelles, entrevues avec le personnel opérationnel clé, essais pour l'évaluation de la vulnérabilité);

c) Intégration de l'équipement fourni par le gouvernement (EFG) et de logiciels pour le regroupement et la surveillance de données sur le réseau;

d) Capacité de respecter les exigences du GC quant à la gestion des incidents de sécurité en collaboration avec le centre de protection de l'information désigné par ce dernier;

e) Capacité d'utiliser les données fournies par le GC pour établir les mesures de protection (p. ex. signature des logiciels malveillants et des intrusions, listes noire et blanche des adresses IP et URL).

Q12 : Décrivez brièvement et de façon générale les différentes stratégies de protection pour l'information de niveau Protégé et l'information de niveau Secret d'une solution de courriel.

Q13 : En ce moment, SPC supporte de multiples réseaux distincts pour le traitement d'information Protégé B et Secret, qui comprennent la messagerie électronique. On estime qu'environ 15 000 utilisateurs se servent de systèmes de courriel qui peuvent traiter de l'information jusqu'au niveau Secret, et qu'environ 377 000 utilisateurs se servent de systèmes pouvant traiter de l'information jusqu'au niveau Protégé B, inclusivement.

a) En vous servant de l'infrastructure existante du GC, pouvez-vous fournir un accès aux systèmes de courriel Protégé B et Secret à partir d'un environnement d'utilisateur commun (p. ex. ordinateur de bureau unique)? Sinon, quelle solution proposez-vous (p. ex. clients légers)?

Dans l'affirmative :

b) Veuillez indiquer les avantages et les inconvénients de la mise en œuvre d'une solution regroupée de courriel qui peut traiter des courriels Protégé B et Secret, plutôt que de deux solutions distinctes, du point de vue des coûts, de la sécurité et de la complexité de l'approvisionnement, des exigences et de la mise en œuvre. Êtes-vous en mesure de fournir une solution regroupée de courriel?

c) Si SPC envisageait d'acquérir deux solutions distinctes, une pour les courriels de niveau Secret et une pour ceux de niveau Protégé B, recommanderiez-vous au Canada de recourir à un seul fournisseur, ou encore à deux fournisseurs, soit un pour chaque solution? Veuillez indiquer les avantages et les inconvénients et formuler vos commentaires quant à la sécurité et à la complexité de l'approvisionnement, des exigences et de la mise en œuvre.

Q14 : Le Canada souhaite que la solution de courriel comprenne des contrôles rigoureux pour tous les dépôts de données du Canada (comme il est décrit à la section 13.5 de la partie III). Ces contrôles doivent aussi comprendre des fonctions de journalisation, de surveillance, de vérification et de rapport détaillés permettant de savoir qui a accédé ou essayé d'accéder aux données de courriels du Canada.

a) Quelles mesures de contrôle (solutions, fonctionnalités, outils, processus, etc.) proposez-vous pour satisfaire à ces exigences?

b) Quelle serait votre façon de procéder pour les sites à l'étranger (p. ex. les missions)? Existe-t-il des limites techniques et des effets sur la prestation de services et le coût dont le Canada devrait tenir compte?

c) Avez-vous d'autres idées ou opinions sur la façon dont le Canada peut protéger la souveraineté de ses données tout en atteignant les objectifs énoncés au point 4.1.5 de la partie II de la présente DDR?

Q15: Avez-vous déjà déployé avec succès une :

a) une solution de courrier électronique de niveau Secret (p. ex. plus de 500 boîtes aux lettres);

b) une solution de courrier électronique de niveau Protégé B;

qui a été attestée selon des normes qui répondraient à celles du GC? Pouvez-vous nous transmettre cette attestation ou une référence? Veuillez expliquer.

14.4 Exigences relatives à la protection des renseignements personnels

Dans la présente section, on demande de l'information sur les considérations liées à la protection des renseignements personnels.

Q16 : Décrivez les processus et les procédures que votre organisation utiliserait pour protéger les renseignements personnels. Veuillez indiquer, précisément, les rôles et les responsabilités, les outils, les ressources, les politiques, les procédures et les pratiques exemplaires que vous utiliseriez pour cette protection.

Q17: Les services de messagerie électronique relaient, reçoivent et conservent une grande quantité de renseignements personnels. Une initiative visant à regrouper la solution de courriel à l'échelle des organisations partenaires présenterait des risques importants pour la confidentialité. Décrivez les stratégies d'atténuation des risques que

votre organisation proposerait pour tenir compte des tendances actuelles en matière de menace à la confidentialité dans une solution de courriel.

14.5 Considérations liées à la plateforme technologique

Dans la présente section, on demande de l'information sur les considérations liées à la plateforme technologique de la solution de courriel.

Q18 : Selon vous, pour quelles composantes ou quels processus de la messagerie électronique (y compris l'infrastructure) le GC devrait-il rester responsable de la prestation de services?

Q19 : Votre solution de courriel serait-telle en mesure d'exploiter les investissements actuels du Canada dans le matériel, les logiciels et les outils (c.-à-d. l'EFG), là ou il y a lieu, de manière à offrir le meilleur rapport qualité-prix? Plus précisément, quelles sont les recommandations de l'industrie quant à la méthode d'évaluation des soumissions potentielles sur la base du coût total de possession (soit le total des coûts de migration, d'intégration et de formation)?

Q20 : En ce moment, les ministères et organismes possèdent de multiples annuaires, y compris des annuaires uniquement pour les courriels, qui ne sont pas intégrés. Comment prévoyez-vous satisfaire à l'exigence de gestion des profils d'utilisateur, des justificatifs d'identité, de l'authentification et de l'autorisation pour la solution de courriel regroupée? Que suggérez-vous au Canada de faire, au chapitre de la gestion des comptes et des annuaires, pour préparer son intégration à la solution d'annuaire de votre service de messagerie électronique?

Q21 : L'ITSC ne prévoit pas la mise au point d'une solution globale de gestion de l'identité, des justificatifs d'identité et de l'accès. Toutefois, si vous connaissez très bien le marché ainsi que les solutions de cette nature utilisées par le GC à l'heure actuelle, pouvez-vous suggérer des stratégies envisageables pour répondre, de façon économique et opportune, aux besoins élémentaires d'une telle solution dans le cadre de l'ITSC?

Q22 : Pour l'instant, chaque ministère ou organisme partenaire gère son propre environnement de bureautique. La majorité des partenaires possèdent habituellement une solution d'accès sécurisé à distance. Les utilisateurs ont souvent un accès mobile à une application de messagerie électronique entièrement fonctionnelle grâce à différentes méthodes comme les clients légers ou les réseaux privés virtuels. Existe-t-il des considérations techniques ou des exigences opérationnelles que le Canada devrait déterminer pour assurer la fourniture de cet accès mobile aux utilisateurs?

Q23 : Le GC aimerait adopter un modèle à identification unique. Avez-vous des suggestions quant à la façon dont l'ITSC peut contribuer à l'atteinte de cet objectif?

Q24 : De quelle façon la solution de courriel pourrait-elle utiliser la technologie des médias sociaux pour la mobilisation et l'habilitation des citoyens?

14.6 Mise en œuvre et migration

Le regroupement des systèmes de courriel utilisés en un seul service de messagerie électronique à l'échelle du GC représente une partie importante de ce projet. Pour le moment, les trois principaux éléments de la migration à l'étude comprennent la migration des données, la migration

des applications (migration du programme et des autres applications qui font actuellement partie des différents systèmes de courriel des divers ministères) et la migration des utilisateurs.

Q25 : Veuillez décrire ce que, à votre avis, le Canada devrait prendre en considération pour la mise en œuvre et la migration en fonction de leçons passées. Mentionnez des leçons apprises dont le Canada devrait tenir compte pour la migration des applications et des données pour un besoin de cette ampleur, de cette portée et de cette complexité.

Q26 : Dans le cadre de vos services de transition, comment assurez-vous la transition de la solution actuelle de vos clients vers votre solution de courriel entièrement développée? Selon vous, quelles sont les principales difficultés de la migration d'au moins 377 000 utilisateurs d'un service de courriel vers la nouvelle solution de courriel? Suggérez-vous au Canada de prendre des mesures pour se préparer à cette migration?

Q27 : Quelles sont les pratiques exemplaires que vous recommanderiez pour la migration d'un grand nombre d'utilisateurs d'un service de courriel à un autre pour que :

a) la migration se déroule le plus harmonieusement possible pour l'utilisateur?
b) les répercussions opérationnelles soient le moins importantes possible pour le GC?
c) les problèmes de compatibilité avec les anciennes applications découlant de la mise en œuvre de la solution de courriel soient réduits au minimum?

Q28 : De quels renseignements auriez-vous besoin à l'étape de l'examen et de la précision des exigences et à l'étape de la demande de soumissions pour estimer avec exactitude le coût de la migration?

Q29 : Que pensez-vous de faire assumer par l'entrepreneur le coût de la formation et de la migration lié au passage de SPC et de ses partenaires de leurs plateformes actuelles à la nouvelle technologie de messagerie électronique?

Q30 : Que pensez-vous des outils d'intégration d'applications et de migration d'interfaces répondant aux normes de l'industrie offerts en ce moment sur le marché?

Q31 : Selon la stratégie actuelle d'intégration, les partenaires de SPC sont chargés d'intégrer leurs applications dans des interfaces normalisées à l'aide de la boîte à outils mise à leur disposition par le fournisseur de la solution de courriel.

(i) Pour éviter les risques liés aux dépendances des partenaires de SPC, quels sont les avantages et les inconvénients de modifier cette stratégie afin de rendre le fournisseur de la solution de courriel responsable de l'intégration de l'application?

(ii) Avez-vous d'autres stratégies que le GC devrait envisager pour réduire les risques (en matière de coûts et de délais) liés à cette intégration?

Q32 : SPC s'intéresse aux leçons apprises dans le cadre de mises en œuvre semblables de services de courriels. Veuillez nous indiquer les leçons que vous avez tirées de projets de services de courriels d'une ampleur, d'une portée et d'une complexité semblables que votre organisation a mis en œuvre dans le passé (dans le cadre duquel votre organisation a regroupé les logiciels de

messagerie électronique de divers fournisseurs, comme Microsoft Exchange, IBM Lotus et Novell GroupWise).

14.7 Gestion des services et opérations

Pour un besoin de cette nature, le GC précise habituellement des niveaux de service. Il inclura probablement une exigence lui permettant de s'assurer qu'il conclut un marché avec un fournisseur de services qui respecte ou dépasse régulièrement les niveaux de service qu'il s'engage à fournir à ses clients.

Q33 : Offrez-vous différents niveaux de service? Le cas échéant, veuillez les décrire. Quels sont les principaux facteurs de coût à chacun de ces niveaux.

Q34 : Quelle segmentation de la collectivité des utilisateurs du GC recommanderiez-vous pour réduire au minimum les coûts de mise en œuvre, de migration et de soutien continu?

Q35 : Pouvez-vous nous faire connaître les paramètres que vous avez utilisés pour la prestation de services et les niveaux de service pour un important projet semblable dans le cadre duquel vous avez fourni un service de courriel? Veuillez donner des exemples de données statistiques précises sur le rendement des services que vous jugez pertinentes pour mesurer la capacité d'un fournisseur à fournir des services de grande qualité.

Q36 : L'entrepreneur devra intégrer les processus et les outils de GSIT de SPC et de ses partenaires. Avez-vous des suggestions pour l'organisation du modèle de service?

Q37 : Dans le modèle de prestation de services choisi à terme, il est possible que la solution globale de courriel soit assurée par plus d'un fournisseur (un pour les services d'applications de courrier électronique, un pour le stockage, un pour le centre d'aide de premier niveau, etc.). Avez-vous des recommandations à formuler quant à la façon dont le GC doit définir et gérer le modèle global de services pour que les responsabilités de chaque fournisseur (relativement au tri, à la résolution des problèmes, à la préparation des rapports de performance, par exemple) soient claires et bien comprises, et pour que le GC puisse en assurer la surveillance?

14.8 Aspects liés à l'écologisation

Le Bureau de l'écologisation des opérations gouvernementales (BEOG) se livre à toutes sortes d'activités. Il établit les priorités, les responsabilités, les cibles, les échéances et les exigences de signalement à l'échelle du gouvernement pour aider ce dernier à respecter son engagement de devenir un modèle d'excellence environnementale dans le cadre de ses propres activités.

Q38 : Votre entreprise a-t-elle une politique environnementale? Le cas échéant, pouvez-vous nous la transmettre ?

Q39 : Nous demandons aux répondants de formuler leurs commentaires sur l'applicabilité et les normes en place ou prévues pour les services gérés de courriel qui s'harmoniseraient avec la stratégie de développement durable (d'achats écologiques) du Canada et l'appuieraient.

14.9 Aspects socioéconomiques liés aux petites et moyennes entreprises

Le gouvernement souhaite appuyer le développement de petites et moyennes entreprises (PME) novatrices au Canada.

Q40 : Que pensez-vous du fait d'exploiter l'ITSC pour appuyer le développement des PME canadiennes novatrices? Comment SPC peut-il contribuer à l'atteinte de cet objectif? Comment peut-il tirer profit du Programme canadien pour la commercialisation des innovations (PCCI)[21] de TPSGC?

Q41 : Si vous êtes un important fournisseur de services de TI, votre modèle d'affaires comprend-il la sous-traitance de parties du travail à de petites entreprises ou à des entreprises régionales? Dans l'affirmative, dans le présent contexte, pour quelles parties des travaux suggérez-vous la sous-traitance à des tiers? Sinon, pourquoi choisissez-vous de ne pas recourir à des sous-traitants ?

Q42 : Si vous êtes une petite entreprise ou une entreprise régionale ou spécialisée, travaillez-vous souvent comme sous-traitant pour de grandes organisations?

Q43 : Selon vous, quels autres services connexes pourraient être fournis par des organisations privées à l'extérieur du cadre de l'ITSC, et qui concerne la conception, la conversion, la transition et la gestion continue du système du service de courriel, ainsi que la facilitation?

14.10 Approche d'approvisionnement proposée

14.10.1 Le processus de SAC est décrit à la section 5 de la partie II – Donnés fondamentales sur l'ITSC. Il s'agit de l'approche d'approvisionnement proposée pour l'ITSC.

Q44 : Connaissez-vous le processus d'approvisionnement novateur? Dans l'affirmative, veuillez formuler des commentaires sur cette approche d'approvisionnement.

Q45 : Le rapport Jenkins [22] recommande que les demandes de propositions, s'il y a lieu, définissent les besoins à satisfaire et les problèmes à régler plutôt que d'adopter une démarche trop contraignante pour la solution. Le Canada compte appliquer cette approche. Êtes-vous d'accord avec cette recommandation? Avez-vous des suggestions quant à la façon dont la recommandation pourrait être mise en œuvre en tenant compte de l'approche de SAC?

14.10.2 Veuillez vous reporter à l'annexe D – Procédures d'évaluation et détermination des répondants retenus.

Q46 : Veuillez indiquer tout commentaire sur les critères d'évaluation obligatoires et cotés présentés à l'annexe D et indiquer les critères que vous trouvez les plus pertinents et les moins pertinents.

---

[21] https://achatsetventes.gc.ca/initiatives-et-programmes/programme-canadien-pour-la-commercialisation-des-innovations-pcci

[22] http://rd-review.ca/eic/site/033.nsf/vwapj/R-D_InnovationCanada_Final-fra.pdf/$FILE/R-D_InnovationCanada_Final-fra.pdf

Veuillez indiquer quels critères vous trouvez les plus pertinents et expliquer votre réponse. Avez-vous d'autres critères à suggérer? Pensez-vous que la meilleure façon d'évaluer ces critères est au moyen d'exigences obligatoires ou cotées (comme le décrit l'annexe D)?

14.10.3 Les services de courriels gérés de grande qualité dépendent largement des compétences des membres de l'équipe de base qui participent à la conception, à l'architecture, à l'élaboration et à la mise en œuvre de la solution de courriel.

Q.47 : SPC s'attend à ce que les répondants retenus présentent une équipe de base pour la mise en œuvre de la solution de courriel. Elle doit être composée des ressources suivantes :

a) Directeur principal de projet;

b) Gestionnaire principal de projet;

c) Analyste des opérations;

d) Architecte technique des systèmes de courriel;

e) Spécialiste principal en conception de la sécurité de la TI;

f) Gestionnaire de mise en œuvre.

Croyez-vous que les compétences des ressources de l'équipe de base présentées à l'annexe A – Glossaire englobent les compétences nécessaires pour l'ITSC?

14.10.4 Le Canada entend recueillir des commentaires sur l'établissement des coûts et des prix concernant le service lié à l'ITSC. On doit indiquer des références précises sur les facteurs déterminant les coûts et les prix et la manière dont ils influent sur le modèle de prix de SPC.

Q48 : Veuillez faire part de vos commentaires sur les modèles d'établissement des prix qui se sont révélés utiles dans le cadre des marchés de services de courriels que vous avez conclus avec d'importantes organisations clientes. Proposez-vous à votre clientèle plus d'un modèle d'établissement des prix lorsque vous fournissez des services gérés ou impartis de courriel? Pouvez-vous en décrire le mode de facturation (c.-à-d. boîte de courriel, utilisateur, etc.)?

Q49 : Selon les exigences opérationnelles obligatoires prévues (décrites à la partie III – Exigences obligatoires prévues) et les renseignements que contient la présente DDR, veuillez fournir les renseignements sur l'établissement des prix concernant vos services de courriels. Ces renseignements serviront à la planification des projets.

Q50 : En quoi votre structure de prix serait-elle touchée si SPC envisageait de fractionner les exigences relatives en matière de courriel dans un système de niveau Secret (incluant renseignements de niveau Classifié jusqu'au niveau Secret et renseignements Protégés jusqu'au niveau Protégé C) et/ou un système Protégé jusqu'au et incluant le niveau Protégé B.

Q51 : Le Canada envisage actuellement de conclure un marché de cinq ans assorti de trois périodes optionnelles de un an chacune. Il comprend la période de mise en œuvre et

de migration. Selon vous, quelle durée de marché (nombre d'années fixes et optionnelles) procurerait au Canada la meilleure tarification de services et profiterait aux deux parties? Veuillez commenter (c.-à-d. l'ampleur des réductions à long terme). S'il s'agit d'une fourchette de réductions, justifiez la durée minimale et la durée maximale du marché.

Q52 : Sur la base des projets de services de courriels de l'envergure de l'ITSC que vous avez déjà réalisés, pouvez-vous présenter la part approximative, en pourcentage, occupée par chacun des grands éléments du coût total de possession sur cinq ans (mise en œuvre, licences d'utilisation des logiciels, serveurs, stockage, opérations, etc.)?

Q53 : Quelles sont les clauses et les conditions uniformisées des offres et des produits de service de courriel gérés, impartis et autres que vous fournissez?

Q54 : Quelle clause uniformisée de limitation de responsabilité appliquez-vous dans le cas d'un projet de la portée et de l'envergure de l'ITSC?

Q.55 : Le GC a l'objectif de réduire au minimum le risque d'une atteinte à la sécurité ou à la vie privée causée par un fournisseur négligent, ou encore par un fournisseur cédant aux pressions d'un État étranger le poussant à livrer le contenu des courriels dont le GC est propriétaire. Pour atteindre cet objectif, que pensez-vous de l'idée d'une responsabilité illimitée?

ANNEXES

ANNEXE A : GLOSSAIRE

1. Sigles

Sigles	Description
AE	Architecture d'entreprise
AIPRP	Accès à l'information et protection des renseignements personnels
ANS	Accord sur les niveaux de service
API	Interface de programmation d'applications
BDITI	Bibliothèque de données sur l'infrastructure des technologies de l'information
BGF	Bureau de gestion des fournisseurs
CalDAV	Calendaring Extensions to Distributed Authoring and Versioning
COTS	Logiciel commercial
DDR	Demande de renseignements
DP	Demande de propositions
DRPE	Demande de réponses pour l'évaluation
EE	Énoncé des exigences
GC	Gouvernement du Canada
GI	Gestion de l'information
GSTI	Gestion des services de TI
HTTPS	Protocole de transfert hypertexte sécurisé
ICP	Infrastructure à clés publiques
IMAP4	Protocole d'accès message Internet (version 4)
ITSC	Initiative de transformation des services de courriels
LAC	Licence d'accès client
LO	Langues officielles
MIME	Extension polyvalente de courrier Internet
MS	Microsoft
MTE	Matrice de traçabilité des exigences
PAAA	Protocole allégé d'accès annuaire
PME	Petites et moyennes entreprises
POP3	Protocole POP (version 3)
RE	Réseau étendu
RM	Réseau métropolitain
RPP	Rapports sur les plans et les priorités
RSS	Format RSS
S/MIME	Extension S/MIME

SAC	Solutions d’approvisionnement collaboratif
SCD	Services des centres de données
SGDDE	Système de gestion des documents et des dossiers électroniques
SGDDI	Système de gestion des dossiers, des documents et de l'information
SMTP	Protocole d’accès simple aux objets
SOAP	Protocole SOAP (Simple Object Access Protocol)
SPC	Services partagés Canada
SPICT	Services professionnels en informatique centrés sur les tâches
SPTS	Services professionnels centrés sur les tâches et les solutions
SRM	Service réseau métropolitain partagé
SRT	Structure de répartition du travail
TI	Technologie de l'information
TPSGC	Travaux publics et Services gouvernementaux Canada
TSSC	Transformation, stratégie de service et conception
WSDL	Langage de description des services Web
XMPP	Protocole extensible de présence et de messagerie

2. Définitions

Terme	Définition
Attestation	Veuillez vous reporter à la définition d'*évaluation de sécurité* (plus loin).
Coentreprise	Association d'au moins deux parties qui mettent en commun leurs fonds, leurs biens, leurs connaissances, leur expertise ou d'autres ressources dans une entreprise commerciale conjointe, parfois appelée consortium, en vue de présenter ensemble une demande visant un besoin.
Projet organisationnel complexe	Mise en œuvre d'une solution de courriel dans une entreprise comportant de nombreux intervenants (au moins 10 000 utilisateurs). Une telle solution y a été intégrée avec de multiples applications opérationnelles.
Équipe de base	Directeur principal de projet La ressource proposée doit avoir acquis, au cours des 15 dernières années, au moins 5 ans d'expérience comme membre principal d'une équipe de projet intégré lors de l'exécution de projets de transformation des services de courriels destinés à une entreprise évoluant dans un projet organisationnel complexe. Gestionnaire principal de projet La ressource proposée doit avoir acquis, au cours des 15 dernières années, au moins 5 ans d'expérience comme gestionnaire principal de projet. Comme membre d'un bureau de gestion des projets, elle doit avoir participé à l'exécution de projets de transformation des services de courriels dans une entreprise évoluant dans un projet organisationnel complexe. Spécialiste principal en conception de la sécurité de la TI[23] La ressource proposée doit avoir acquis, au cours des 15 dernières années, au moins 10 ans d'expérience à ce titre. Elle doit également avoir participé à un minimum de 2 projets de transformation opérationnelle des services de courriels, au cours desquels elle réalisait, sur la base du contenu de la proposition technique du soumissionnaire (p. ex. solution de courriel Protégé B ou Secret, combinaison de solutions de courriel), les

[23] On peut trouver de plus amples renseignements sur cette catégorie de resources sur le site Web du service Arrangement en matière d'approvisionnement en cyberprotection (AMAC) à l'adresse suivante : http://www.tpsgc-pwgsc.gc.ca/app-acq/amac-cpsa/ws3-fra.html.

	activités suivantes : (i) Établissement des exigences relatives à la sécurité et des matrices de traçabilité dans un projet organisationnel complexe; (ii) Préparation de rapports techniques : analyse des besoins, analyse des possibilités, documents d'architecture technique (architecture de sécurité, entre autres), etc.; (iii) Conception de solutions de courriel sécuritaires, notamment de solutions de sécurité pour les courriels mêmes et les applications connexes, les serveurs Web et serveurs de base de données, les répertoires et les composants réseau; (iv) Établissement des exigences opérationnelles relatives à la sécurité au cours de la période de fonctionnement et de la période de mise hors service de la solution de courriel. Gestionnaire de mise en œuvre La ressource proposée doit avoir acquis, au cours des 15 dernières années, au moins 5 ans d'expérience comme gestionnaire de mise en œuvre dans des projets de transformation des services de courriels réalisés dans une entreprise évoluant dans un projet organisationnel complexe. Architecte technique des systèmes de courriel La ressource proposée doit avoir acquis, dans les 15 dernières années, au moins 5 ans d'expérience comme architecte technique des systèmes de courriel dans des projets de transformation des services de courriels réalisés dans une entreprise évoluant dans un projet organisationnel complexe. Analyste des opérations La ressource proposée doit avoir acquis, au cours des 10 dernières années, au moins 3 ans d'expérience comme analyste des opérations dans des projets relatifs aux TI réalisés dans une entreprise évoluant dans un projet organisationnel complexe.
Organisation cliente	Entité d'au moins 5 000 utilisateurs issus d'une organisation privée ou publique. Ces utilisateurs utilisent une solution de courriel conçue, structurée, développée et mise en œuvre par le répondant.

Partenaires	Ministères et organismes bénéficiaires des services de technologie de l'information (TI) offerts par SPC. On en trouve la liste complète à l'annexe E.
Partie intéressée	Organisation qui souhaite participer aux activités de l'étape de la consultation de l'industrie liées à l'ITSC.
Plateforme	Composantes polyvalentes de systèmes d'information servant à traiter et à stocker des données électroniques (ordinateurs de bureau, serveurs, dispositifs de réseau et appareils mobiles). Les plateformes sont en général constituées de logiciels (systèmes d'exploitation, pilotes de périphérique et applications).
Protocole de communications par courriel IMAP	Veuillez consulter le RFC 3501 - http://tools.ietf.org/html/rfc3501.
Renseignements classifiés	Font référence à l'intérêt national. Ils portent sur la défense et le maintien de la stabilité sociale, politique et économique du Canada. Il existe trois niveaux de renseignements classifiés. Très secret : l'atteinte à l'intégrité d'un nombre très restreint de ces renseignements pourrait causer un préjudice exceptionnellement grave à l'intérêt national. Secret : l'atteinte à l'intégrité de ces renseignements risquerait de causer un préjudice grave à l'intérêt national. Confidentiel : l'atteinte à l'intégrité de ces renseignements risquerait de causer un certain préjudice à l'intérêt national.
Service géré	Prestation d'un service à l'organisation cliente lorsque le fournisseur de la solution de courriel est chargé de la prestation du service en question et que le service doit répondre aux niveaux de service prédéterminés du client.
Service imparti	Lorsque la définition, la construction, la migration et l'exploitation de la nouvelle solution de courriel relèvent exclusivement d'un fournisseur de solutions de courriel du secteur privé. L'infrastructure lui appartient et est administrée par lui. Le service est situé dans des centres de données gérés par le fournisseur de solutions de courriel.
Service interne	Une solution de courriel conçue et mise en place par des ressources techniques internes de SPC.
Solution de courriel	Une solution de courriel peut comprendre un ou plusieurs systèmes ou centres de données de TI, un ou plusieurs réseaux de communication, des serveurs, des applications client, des applications serveur, etc. Ces éléments peuvent être mis en œuvre, utilisés et gérés dans un environnement propre au GC ou comme service offert par un fournisseur de service commercial.

Solution regroupée	Signifie que la solution d'ITSC choisie satisfera à toutes les exigences de SPC et de ses partenaires en matière de courriel.
Solutions d'approvisionnement collaboratif	Approche d'approvisionnement collaboratif formée des étapes suivantes : i. Étape de consultation de l'industrie : obtenir les commentaires de l'industrie sur l'approche relative au projet et à l'approvisionnement. ii. Étape de la DRPE : identifier les répondants retenus. iii. Étape de l'examen et de la précision des exigences : les répondants retenus collaborent avec SPC pour examiner et peaufiner les exigences opérationnelles et techniques relatives au courriel. iv. Étape de la demande de soumissions : les répondants retenus sont invités à présenter leurs propositions techniques et de prix. v. Étape de l'attribution du marché : attribuer le marché au(x) soumissionnaire(s) retenu(s). vi. Étape de mise en œuvre : conception de l'architecture, développement et mise en œuvre de la solution de courriel et prestation des services.
Soumissionnaire	Personne ou entité (ou, dans le cas d'une coentreprise, les personnes ou les entités) qui présente une soumission pour l'exécution d'un marché de biens, de services ou les deux. Le terme ne comprend pas la société mère, les filiales ou autres affiliées du soumissionnaire, ni ses sous-traitants.

Renseignements protégés	Font référence à des dispositions particulières de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels.* Ils s'appliquent aux renseignements personnels de nature délicate, aux renseignements sur la vie privée et aux renseignements commerciaux. Protégé A (renseignements de nature peu délicate) : s'applique aux renseignements pour lesquels toute atteinte à l'intégrité des renseignements risquerait vraisemblablement de porter préjudice à des intérêts autres que l'intérêt national, p. ex. la divulgation du salaire exact. Protégé B (renseignements de nature particulièrement délicate) : s'applique aux renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice sérieux à des intérêts autres que l'intérêt national, p. ex. la perte de réputation ou d'avantage concurrentiel. Protégé C (renseignements de nature extrêmement délicate) : s'applique à un nombre très restreint de renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice extrêmement grave à des intérêts autres que l'intérêt national, p. ex. la perte de vie.
Demande de réponses pour l'évaluation (DRPE)	Instrument d'achat servant à identifier des répondants retenus pour l'étape de l'examen et de la précision des exigences et pour l'étape de la demande de soumissions de l'approche d'approvisionnement des SAC.
Répondant	Organisation qui présente une réponse écrite (dans des documents électronique) à une DDR ou à une DRPE.
Évaluation de sécurité	Processus continu d'évaluation du rendement des contrôles de sécurité de TI au moyen du cycle de vie des systèmes d'information. Ce processus vise à établir la mesure dans laquelle les contrôles sont mis en œuvre adéquatement, fonctionnent comme prévu et produisent les résultats voulus pour ce qui est de répondre aux besoins opérationnels des ministères en matière de sécurité. L'évaluation de la sécurité soutient l'autorisation en donnant des raisons d'avoir confiance à la sécurité du système d'information.

Autorisation de sécurité	Processus continu consistant à obtenir et à maintenir une décision officielle de gestion prise par un cadre supérieur de l'organisation. Ce processus vise autoriser l'exploitation d'un système d'information et à accepter expressément le risque d'en dépendre pour appuyer un groupe d'activités opérationnelles fondé sur la mise en œuvre d'un ensemble de contrôles de sécurité faisant l'objet d'un consensus et sur les résultats de l'évaluation de sécurité régulière.
Posture de sécurité	Caractéristique d'un système d'information correspondant à la capacité des contrôles de sécurité mis en œuvre pour répondre aux besoins opérationnels à ce chapitre et neutraliser un environnement risqué choisi. Nota : Une posture de sécurité qui répond aux besoins opérationnels de sécurité et qui neutralise un environnement risqué choisi est jugée *adéquate*. La posture de sécurité peut évoluer au fil du temps, à mesure qu'évoluent les menaces et les besoins opérationnels et que l'on découvre des points vulnérables. Le maintien d'une posture de sécurité adéquate nécessite d'examiner et d'actualiser les contrôles de sécurité mis en œuvre pour les adapter aux changements. Nota : La posture de sécurité d'un système d'information est évaluée avec la même méthodologie qui sert à évaluer les risques de sécurité. Il s'agit donc d'un concept étroitement lié. Le caractère adéquat d'une posture de sécurité suppose des risques résiduels faibles.
Service	Service fourni à un ou à plusieurs clients par un fournisseur de services de TI. Un service de TI repose sur l'utilisation de la TI et soutient les processus opérationnels du client. Un service de TI est conçu grâce à une combinaison de personnes, de processus et de technologies. Il doit être défini dans un accord sur les niveaux de service (ANS) (3^{e} version du glossaire de la BDITI). Nota : Le service est un moyen d'apporter une valeur ajoutée aux clients en contribuant aux résultats qu'ils souhaitent obtenir sans assumer de risques ni de coûts particuliers.
Protocole de communications par courriel SMTP	Veuillez consulter le RFC 5321 - http://tools.ietf.org/html/rfc5321.
Répondant retenu	Répondant choisi par le Canada pour participer à l'étape de l'examen et de la précision des exigences et à l'étape de la demande de soumissions de l'approvisionnement.

Menace à l’approvisionnement	On peut facilement trafiquer un produit dans la chaîne d’approvisionnement afin de faciliter par la suite une cyberattaque contre lui pour exploiter un réseau et les renseignements qui y circulent. Pour remporter des marchés portant sur des initiatives de services partagés de TI du GC, les fournisseurs de solutions de courriel doivent satisfaire aux exigences de sécurité liées à la cyberprotection, à la cyberdéfense et à l'atténuation des risques liés à la l'approvisionnement.
Système	Terme générique désignant le réseau et d’autres dispositifs, des systèmes d’exploitation, des plateformes, des logiciels et des applications de virtualisation ou toute combinaison de ces éléments. Son utilisation est propre à un contexte.

ANNEXE B : MATRICE SUR LA PORTÉE DE L'ITSC

La portée fonctionnelle générale est définie ci-dessous. Les éléments précis de la portée et les exigences sous-jacentes (c'est-a-dire l'harmonisation avec la vision et la stratégie, l'utilisation des normes et l'intégration avec les services actuels de SPC) seront affinés et documentés de façon plus détaillée pendant l'étape de l'examen et de la précision des exigences.

N° de réf.	Portée	Dans la portée	Hors de portée	Interface seulement	Observations
1.	Courriels				
	Fonctionnalité de messagerie par courriel standard	X			Supporte la fonctionnalité de messagerie par courriel propre à tous les grands logiciels commerciaux (COTS).
	Accès à l'historique des courriels	X			Permet aux utilisateurs d'accéder à l'historique de leurs courriels (actifs et archivés) à l'aide de la nouvelle solution de courriel. L'accès sera restreint selon la période de conservation établie pour SPC et ses partenaires.
	Intégration télécopieur			X	Supporte l'interface destinée aux services centraux et à la fonctionnalité de télécopieur.
	Plateformes physiques mobiles		X		La capacité de courriel pour les environnements dotés d'une mobilité physique est hors de portée (ex. : déploiements militaires, navires militaires).
2.	Gestion des calendriers/calendrier				
	Fonctionnalité standard de gestion des calendriers	X			Supporte la fonctionnalité typique de gestion des calendriers et de calendrier propre à tous les grands logiciels commerciaux
	« Free/Busy Look-up » pour les utilisateurs du système commun de courriel	X			Permet aux utilisateurs de consulter des calendriers (« free/busy availability ») et de prévoir des réunions avec d'autres utilisateurs au moyen du système commun de courriel.
	« Free/Busy Look-up » pour les utilisateurs qui ne se trouvent PAS sur le système commun de courriel.		X		
3.	Gestion des contacts				
	Fonctionnalité de gestion des contacts standard	X			Supporte la fonctionnalité de suivi des contacts propre à tous les grands logiciels commerciaux.

N° de réf.	Portée	Dans la portée	Hors de portée	Interface seulement	Observations
4.	Gestion des appareils mobiles				
	Soutien des appareils mobiles (les téléphones intelligents BlackBerry[MD] et les tablettes Playbook de RIM, les tablettes iPad[MD] et les téléphones intelligents iPhone d'Apple, les téléphones intelligents et les tablettes Android[MD], etc.)	X			Permet aux utilisateurs d'accéder à la fonctionnalité standard de courriel et de gestion des calendriers au moyen de ces appareils. L'ampleur du support varie d'un appareil à l'autre selon les capacités et les contraintes de chacun.
5.	Annuaire				
	Annuaire de courriels	X			Permet aux utilisateurs de trouver n'importe quel autre utilisateur du GC dans le répertoire de courriels commun grâce à la solution de services de carnet d'adresses.
	Gestion des listes de distribution	X			Permet de créer et de gérer les listes de distribution pour simplifier la communication avec les groupes de destinataires.
6.	Outils de collaboration				
	Messagerie instantanée	X			Une solution de messagerie instantanée sera mise en œuvre et offerte à tous les utilisateurs de la solution commune de courriel.
	Support d'autres caractéristiques de collaboration : espaces de travail collaboratif, conférences Web, partage d'applications, intégration de la messagerie vocale dans les courriels, forums de discussion, wikis et blogues		X	X	Les technologies et les services de collaboration et de communications unifiées sont hors de portée. Toutefois, l'éventuelle capacité d'intégration dans ces technologies et services demeure dans la portée.
7.	Exigences de sécurité				
	Antivirus/anti-pollupostage	X			Supporte la fonctionnalité d'antivirus et d'antipollupostage standard pour la messagerie propre à tous les grands logiciels commerciaux.
	Le GC définit l'interface de gestion de justificatifs d'identité			X	Le service regroupé de courriel comportera une fonctionnalité de cryptage et d'ICP. Les travaux à effectuer seront cependant traités en dehors des exigences de la présente initiative.

N° de réf.	Portée	Dans la portée	Hors de portée	Interface seulement	Observations
	Capacité de courriel Secret	X			Présente une capacité de courriel secret pour un sous-ensemble d'utilisateurs de SPC.
8.	Intégration des applications				
	Interfaces de programmation d'applications (API) pour courriel	X			Fournit une interface conforme aux normes de l'industrie pour que les applications puissent envoyer et recevoir des courriels (voir le point 10, Soutien « normes ouvertes » pour en savoir plus).
	API standards pour la gestion de calendriers	X			Fournit une interface conforme aux normes de l'industrie pour que les applications puissent envoyer et recevoir des calendriers (voir le point 10, Soutien « normes ouvertes » pour en savoir plus).
	API standard pour les contacts	X			Fournit une interface répondant aux normes de l'industrie pour que les applications puissent envoyer et recevoir des renseignements sur les contacts (voir le point 10, Soutien « normes ouvertes » pour en savoir plus).
	Intégration des applications existantes dans le nouveau système commun de courriel			X	Cet aspect incombe au ministère. SPC fournira une interface et appuiera ses efforts d'intégration et ceux de ses partenaires.
	Support et documents techniques destinés à SPC et à ses partenaires pour l'intégration des applications	X			SPC fournira une interface et appuiera ses efforts d'intégration et ceux de ses partenaires.
9.	Sauvegarde et archivage				
	Planification des urgences (ex. : reprise après sinistre ou après défaillance)	X			Capacité à récupérer les capacités de courriel dans diverses situations de sinistre ou de défaillance.
	Archivage de courriels	X			Supporte l'archivage de courriels et la capacité, pour l'utilisateur, de récupérer facilement des courriels archivés de manière automatisée.
	Sauvegarde et restauration des boîtes aux lettres	X			Capacité à sauvegarder et à restaurer les courriels (pour l'ensemble des boîtes aux lettres, par groupe et par boîte aux lettres).

N° de réf.	Portée	Dans la portée	Hors de portée	Interface seulement	Observations
	Intégration dans les outils de gestion de l'information (comme le système de gestion des documents et des dossiers électroniques [SGDDE], le système de gestion des dossiers, des documents et de l'information [SGDDI] et GCDocs)			X	Le service de courriel sera intégré dans une solution de SGDDE. L'ITSC n'est toutefois pas chargée de l'établissement ou du développement de la solution.
10.	Autres exigences ou contraintes techniques				
	Support « normes ouvertes »	X			Supporte les normes ouvertes permettant l'interopérabilité de différentes composantes de messagerie. Les normes particulières à supporter comprennent notamment : HTTPS, POP3 par rapport au protocole TLS, IMAP par rapport au protocole TLS, SMTP par rapport au protocole TLS, PAAA, CalDAV, CalDAV par rapport au protocole TLS, XMPP, format RSS, OMA-DS, P-IMAP, WebDAV, WebDAV par rapport au protocole TLS, PAAA par rapport au protocole TLS, VoiceXML, SOAP, MIME, S/MIME et soutien délégué pour les cadres d'authentification externes.
	Formation des utilisateurs	X			Des documents pédagogiques et de formation en ligne seront disponibles. En outre, la solution de courriel préparera des documents de formation à l'intention des utilisateurs et formera les formateurs au cours de la période de transition.
	Ouverture de session unique/ouverture de session simplifiée	À déterminer	À déterminer	À déterminer	SPC aimerait éventuellement passer à un modèle d'ouverture de session unique. Durant l'étape de la consultation de l'industrie, SPC déterminera si l'ITSC peut atteindre cet objectif.
11.	Exigences de migration				
	Migration des courriels et des contacts	X			Migration, vers le nouvel environnement, du contenu des courriels existants et des contacts.

N° de réf.	Portée	Dans la portée	Hors de portée	Interface seulement	Observations
	Migration des calendriers	X			Migration, vers le nouvel environnement, des calendriers assortis de délais précis.
12.	Établissement du service				
	Embauche d'un fournisseur de service de courriel du secteur privé	X			
	Assurance de l'exécution d'un cadre de gestion de service continu	X			Modèle de référence pour définir un cadre de gestion de service : consulter la 3e version de la BDITI.

ANNEXE C : SOMMAIRE DE L'ÉTAT ACTUEL

1. Aperçu des services de courriels actuels du GC

1.1 Problèmes d'architecture

Le GC héberge de nombreux systèmes de courriel constitués d'une foule d'architectures, de conceptions, de produits et de processus de gestion. Ils représentent une part importante de la vaste empreinte d'infrastructure de TI et sont cruciaux pour les activités opérationnelles du GC.

À l'heure actuelle, diverses infrastructures de TI approvisionnent une multitude de systèmes de courriel au GC. Chaque ministère et organisme utilise des versions et des niveaux de lancement différents de même que divers niveaux de maintenance et de sécurité. Chaque système de courriel est acheté séparément ainsi que géré et supporté par les processus de gestion et les modèles de soutien de la TI de chacun des ministères et organismes.

Les éléments suivants expriment avec beaucoup de précision certains des principaux domaines présentant des différences parmi les partenaires de SPC :

- Des mises en œuvre qui, pour l'essentiel, sont considérablement décentralisées présentent différentes architectures, ce qui cause des écarts de fonctionnalité, de rendement et d'interopérabilité. De plus, cela entraîne l'achat et des mises en œuvre inutiles de matériel/logiciels ainsi qu'un chevauchement des fonctions de maintenance, de support et de protection de la sécurité. Voici des exemples de différences d'architecture :
    - Matériel : On trouve dans les centres de données, dans les parcs de serveurs et dans les bureaux locaux partout au pays des centaines de serveurs de fabrication et de modèles différents.
    - Logiciels : On trouve dans les ministères et les organismes une foule de solutions de logiciels de courriel. Ces divers systèmes de courriel ne sont pas entièrement compatibles. Si la majorité des ministères et des organismes utilisent Microsoft Exchange et Outlook, on constate que certains utilisent plutôt IBM Lotus Notes et Novell GroupWise. Les ministères et les organismes ont différentes versions de logiciels et ont adopté une série de processus et de pratiques incompatibles.
    - Versions : On trouve des produits existants et des produits de pointe ainsi que de nombreuses versions.
    - Contrat de licence : Chaque ministère et organisme négocie et gère des contrats de licence distincts.
- La gestion indépendante des infrastructures de fondation (dont les ressources pour les réseaux et pour les centres de données) et le soutien de la TI s'effectuent localement par différents modèles de soutien ministériels et d'organisme (1er, 2e et 3e niveaux). Cet état de fait contribue à modifier les niveaux de service. En voici des exemples :

- Disponibilité
- Procédures de reprise après sinistre
- Procédures de sauvegarde et capacités de reprise
- Politiques de stockage et d'archivage (c.-à-d. capacité, période de conservation)
- Gestion des incidents et des changements
- Objectifs de temps de réponse
- Services de soutien

- Utilisation variable des produits de sécurité (antivirus, antipollupostage, détection d'intrusion, etc.), ce qui entraîne un manque d'uniformité des approches en matière de sécurité et de confidentialité des données.
- Détermination et application individuelles des politiques de courriel (taille des boîtes de courriel, taille des pièces jointes, période de conservation des données, etc.).
- Méthodes et technologies variées servant à intégrer les applications opérationnelles aux systèmes de courriel.

1.2 Fonctionnalités et capacités

En ce qui concerne les services de courriels actuellement disponibles au GC, les fonctionnalités suivantes sont habituellement fournies :

- Courriels
- Contacts
- Gestion de calendriers
- Dossiers publics et partagés
- Tâches
- Notes

Bien que la plupart des systèmes de courriel aient la capacité de fournir les services suivants, il reste encore à déterminer s'ils seront offerts aux partenaires de SPC et s'ils demeureront constamment disponibles pour eux (et, le cas échéant, de quelle manière) :

- Interfaces utilisateur bilingues
- Messagerie instantanée
- Antivirus
- Protection contre les pourriels
- Cryptage
- Intégration du serveur d'entreprise BlackBerry^{MD} (BES)
- Archivage
- Soutien mobile

1.3 Interdépendance des systèmes de courriel

Bien que les systèmes de courriel soient formés d'un certain nombre de composantes d'infrastructure de messagerie particulières, ils dépendent entièrement de plusieurs autres composantes (ou y sont intégrés) pour pouvoir fournir un service de livraison de courriel global. Voici ces composantes :

- Couche présentation du client
- Applications opérationnelles
- Plateforme de sécurité
- Services des annuaires
- Traitement de centre de données
- Capacité de stockage
- Capacité de réseau.

2. Éléments de services de courriels actuels des partenaires de SPC

Les renseignements et les données presentés dans la présente annexe ont été recueillis au moyen de sondages menés par SPC en novembre et décembre 2011 pour le compte de ses partenaires (43 ministères et organismes).

2.1 Résumé des données quantitatives

Le tableau 1 ci-dessous donne un résumé de certaines des données recueillies les plus révélatrices. Étant donné que les sondages ont été réalisés à l'automne 2011, les données ne sont peut-être pas tout à fait représentatives de la situation actuelle.

Description des données	Total partiel	Total
Nombre total de plateformes de services de courriels		3
Nombre total des serveurs de courriel (Lotus – 677; Novell – 159; MS Exchange – 867)		1 703
Nombre total d'employés		377 804
Volume total des courriels stockés (à l'heure actuelle)		950 To
Organisations qui utilisent actuellement les communications unifiées		18
Total des applications ministérielles intégrées par courriel (estimation)		2 250
Nombre de licences Outlook		369 480
Nombre de réseaux		144
Nombre de licences MS Exchange édition standard avec assurance logicielle	354	
Nombre de licences MS Exchange édition standard sans assurance logicielle	125	
Nombre de licences MS Exchange édition entreprise avec assurance logicielle	518	
Nombre de licences MS Exchange édition entreprise sans assurance logicielle	324	
Nombre total de licences de serveur MS		1 321
Nombre de MS Exchange CALs avec assurance logicielle	254 909	
Nombre de MS Exchange CALs sans assurance logicielle	68 965	
Total de MS Exchange CALs		323 874
Nombre de licences Lotus Notes / Domino	23 535	

Number de licences Novell GroupWise	52 392	
Nombre total de licences (Exchange, Notes et GroupWise)		399 801
Nombre de boîtes aux lettres d'utilisateurs	562 270	
Nombre de boîtes aux lettres génériques	75 050	
Nombre total de boîtes aux lettres		637 320
Nombre de téléphones intelligents BlackBerry[MD]	70 167	
Nombre d'autres appareils de télécommunication mobiles	347	
Nombre total des appareils mobiles		70 514

Tableau 1 : Résumé des données quantitatives

Nota

- Le nombre de boîtes aux lettres comprend les boîtes en service et celles qui ne le sont pas. Une boîte peut être mise hors service quand un employé prend sa retraite, a été muté ou a accepté un détachement.
- Le GC a également conclu une entente relative à des licences de logiciel pour Oracle Beehive. Ces licences comprennent un service de messagerie dans un environnement collaboratif.

2.2 Systèmes de courrier électronique

Les ministères et organismes partenaires utilisent 63 systèmes de courriels. Le nombre total de boîtes aux lettres à SPC avoisine les 637 320. Ce chiffre comprend les 562 270 boîtes aux lettres d'utilisateurs et les 75 050 boîtes aux lettres de ressources. Les boîtes aux lettres des cinq plus importantes entités de SPC représentent 59 % de l'ensemble des boîtes aux lettres.

Ces 63 systèmes de courrier électronique se répartissent parmi trois types d'applications logicielles et de systèmes de matériel de soutien :

- Microsoft Exchange (serveur) et Microsoft Outlook (client);
- Novell GroupWise;
- Lotus Notes d'IBM.

Chacun de ces systèmes de courrier électronique est fourni, mis en œuvre, supporté et géré individuellement, et ils sont tous liés à un environnement de serveur BlackBerry[MD] dédié.

Les données statistiques qui suivent définissent la taille globale actuelle du service de courrier électronique de SPC :
Environ 59 % des membres des organisations mandatées de SPC (soit 168 102 personnes) travaillent dans les régions, alors que 41 % (soit 114 898 personnes) travaillent dans la région de la capitale nationale (RCN).

2.3 Appareils de télécommunication mobiles

Les services BlackBerry[MD] font partie intégrante de l'infrastructure de messagerie électronique du gouvernement du Canada. Habituellement, ils fournissent aux utilisateurs de BlackBerry[MD] un accès mobile aux ressources gouvernementales, notamment à un service de messagerie, à un calendrier, à des coordonnées de personnes-ressources, et un accès sans fil à Internet et à l'intranet. Certains ministères et organismes fournissent un accès à des applications administratives ou opérationnelles ministérielles ou en ligne à partir d'un téléphone intelligent BlackBerry[MD] ou d'un autre appareil mobile.

Actuellement, environ 70 514 appareils mobiles (70 167 téléphones intelligents BlackBerry[MD] et 367 autres téléphones intelligents) sont en circulation chez les partenaires de SPC. Les utilisateurs d'appareils mobiles des cinq plus importants ministères et organismes (MDN, Gendarmerie royale du Canada [GRC], ministère des Affaires étrangères et du Commerce international [MAECI], Agence du revenu du Canada [ARC] et Ressources humaines et Développement des compétences Canada [RHDCC]) représentent près 50 % (49,8 %) de l'ensemble des utilisateurs d'appareils mobiles actuellement en circulation.

2.4 Applications mobiles

Actuellement, très peu d'applications opérationnelles ministérielles sont installées sur les appareils mobiles des membres des ministères et organismes partenaires. En fait, seulement sept organisations de SPC (ministère de l'Agriculture et de l'Agroalimentaire [AAC], Santé Canada [SC], RHDCC, Parcs Canada [PC], Bureau du Conseil privé [BCP], Transport Canada [TC] et d Secrétariat du Conseil du Trésor [SCT]) ont installé des applications opérationnelles sur leurs appareils mobiles. Pour ces sept organismes, onze applications de courriel ont été installées sur les appareils mobiles.

2.5 Services d'annuaire

Un service d'annuaire de domaines est un élément d'infrastructure essentiel à tout système de courrier électronique. Cependant, cela n'est pas considéré comme un élément particulier à un système de courriel. En effet, il convient à la plupart, et peut-être même à tous les services distribués, notamment l'identification des utilisateurs ou le contrôle d'accès des utilisateurs. Il s'agit d'un service d'annuaire qui fournit aux utilisateurs de services de courriels un annuaire de tous les employés d'un ministère et un accès à la liste globale d'adresses (GAL) des employés des autres organisations gouvernementales qui ont choisi de mettre en commun leurs annuaires.

En plus de toutes les différences entre les systèmes de courriels du GC, chacun d'entre eux dépend de son propre annuaire ministériel d'adresses électroniques. À l'échelle gouvernementale, il existe environ 700 mises en œuvre d'annuaires (la majorité sont des annuaires actifs Microsoft [MS]) liés à la distribution des systèmes de courrier électronique.

Bon nombre des ministères et d'organismes ont intégré l'ouverture de séance à partir du bureau et l'identification avec accès aux courriels pour permettre la gestion efficace des coûts d'infrastructure, et la plupart, mais pas tous, offrent l'accès direct aux courriels par ouverture de séance à partir du bureau.

Les partenaires de SPC disposent des annuaires d'adresses de courriel mis en œuvre suivants :

- 32 services d'annuaires actifs MS
- 5 services d'annuaires Lotus
- 8 services d'annuaire Novell

Nota : Le nombre total des annuaires mentionnés ci-dessus est de 45 (et non de 43) parce que deux partenaires (Santé Canada [SC] et Industrie Canada [IC]) utilisent deux annuaires. Comme il a été noté précédemment, bon nombre de ces annuaires sont mis en œuvre dans un environnement décentralisé.

2.6 Réseau

Tous les systèmes de courriel du GC dépendent de 144 réseaux de télécommunication sous-jacents et sont supportés par eux. Chacun de ceux-ci est un réseau distinct qui héberge divers services ministériels, notamment la messagerie électronique.

À l'exception des réseaux de certains grands ministères et organismes (Agence des services frontaliers du Canada [ASFC], ARC, MDN ET GRC), la plupart de ces réseaux sont acquis grâce à des marchés communs partagés liés à des services de réseaux convergents du GC. De plus, les partenaires de SPC sont connectés au Réseau de la Voie de communication protégée (VCP), et bon nombre d'entre eux (26) sont déjà connectés au service de réseau métropolitain partagé du GC. Il convient en outre de noter que des ententes de réseautage sont en vigueur (pour certains des partenaires de SPC) pour répondre aux besoins de connexion à l'échelle internationale.

SPC peut tirer parti de l'infrastructure du service de réseau métropolitain partagé du gouvernement et de la connectivité actuelle du ministère pour permettre le déploiement d'un système de courriel regroupé pour tous les employés de SPC au pays. Actuellement, le service de réseau métropolitain n'est offert que dans la RCN, alors que la VCP du GC a une portée internationale.

Les services de courriels sont fournis de manière centralisée, décentralisée ou les deux, selon la capacité du modèle de réseau de chaque ministère et organisme, notamment l'optimisation du réseau étendu, la topologie du réseau, la gestion de la bande passante.

2.7 Stockage

Les systèmes de courrier électronique centralisés dépendent des solutions de stockage des ministères (les réseaux de stockage) qui peuvent stocker une quantité considérable de courriels au même endroit et fournir divers paliers de services à la

clientèle et d'exploitation du stockage à l'archivage en ligne. Bien que la plupart des partenaires de SPC aient recours à des solutions de stockage centralisées, celles-ci sont utilisées très différemment en ce qui a trait aux périodes de conservation des données non structurées et à leur archivage (p. ex. un niveau de stockage principal par rapport à archivage), au retrait en libre-service et aux autres services de stockage. Ainsi, les données d'un sondage mené à l'automne 2011 auprès des 43 ministères et organismes partenaires ne permettent pas de définir clairement l'utilisation réelle de l'outil de stockage.

Par ailleurs, les systèmes de courrier électronique distribués ont tendance à stocker le contenu des clients dans des systèmes de stockage locaux qui coûtent moins cher. Il s'agit habituellement de lecteurs de disques de fichiers locaux et de serveurs d'impression. Quel que soit l'outil de stockage, différentes approches sont adoptées pour stocker les courriels localement (p. ex. les utilisateurs de Microsoft utilisent des tableaux de stockage personnel). Certains ministères et organismes permettent la gestion du stockage de fichiers locaux à même les boîtes aux lettres, ce qui joue sur la quantité de données stockées que les ministères et les organismes signalent comme étant liée aux courriels, alors que d'autres les traitent comme des fichiers personnels stockés.
Les pratiques de stockage et de sauvegarde sont très différentes d'un partenaire de SPC à un autre. Certaines pratiques de stockage permettent de garder les données de trois à cinq ans, ou, dans bien des cas, les organisations conservent leurs dossiers de courriels jusqu'à ce que les utilisateurs quittent l'organisation.

Selon les résultats d'un sondage mené à l'automne 2011, la quantité de courriels stockés actuellement pour les 43 organisations de SPC représente environ 950 téraoctets (To). Environ 60 % (plus ou moins 573 To) des données stockées sont gérées de façon centralisée dans la RCN, alors que 40 % (plus ou moins 377 To) sont gérés localement dans les régions. Des 950 To de données stockées, l'ARC en gère 385 To, soit 40,5 % de la quantité totale des données stockées par les partenaires de SPC. Les cinq organisations qui ont le plus de données stockées (CRA, MAECI, SC, Statistique Canada [StatCan] et RHDCC) comptent pour 58 % du total des données stockées par les ministères et les organismes de SPC. Cependant, le Canada estime que l'espace total de stockage actuellement utilisé par les partenaires de SPC s'élève réellement à 1 600 Po (1,6 pétaoctet) parce que certains partenaires n'ont pas été en mesure de fournir des renseignements sur le PST dans leur rapport.

2.8 Archivage

Environ 44 % des partenaires ont mis en œuvre une solution d'archivage pour leurs courriels. Cependant, les politiques, les directives, les processus et les outils sont très différents d'un ministère à un autre, et il n'existe aucune solution d'archivage normalisée.

2.9 Conservation des données

Aucune caractéristique de courriels ne montre les grandes différences qui existent entre les directives de conservation de données des ministères et organismes partenaires. Alors que certaines organisations gardent leurs données pendant 30 jours, d'autres les conservent pendant 7 ans, et un partenaire a même mentionné qu'il les gardait indéfiniment.

2.10 Protection

Aujourd'hui, le GC dépend grandement de la technologie, ce qui a eu pour effet d'augmenter pour le Canada les risques liés à la perte ou à la manipulation de données et aux comportements inopportuns voulus ou accidentels. Du coup, la nécessité de solutions de protection pour prévenir ou remédier aux risques a lui aussi augmenté.

Tous les courriels sont soumis à des mesures de sécurité conçues pour protéger l'intégrité des données du GC et l'environnement informatique, notamment : des pare-feu, des antivirus, des solutions de détection d'intrusion, de protection contre les pourriels, le contenu inapproprié et la vérification de pièces jointes. Chaque système de courrier électronique de partenaire permet actuellement l'entrée de données Protégé A et Protégé B et de données secrètes, et le ministère ou l'organisme applique son interprétation du niveau de protection requis ce qui comprend, entre autres, divers produits de sécurité, versions de logiciels et solutions de matériel informatique.

En outre, la plupart, si ce n'est la totalité, des ministères et des organismes ont mis au point des politiques rigoureuses relativement à la mise en œuvre de solutions d'ICP exigeant un certificat d'utilisateur unique pour le chiffrement des messages électroniques et des capacités de signature numérique.

Dans le sondage, tous les partenaires de SPC ont déclaré avoir de nombreux systèmes pour protéger leurs systèmes de courriel, notamment des programmes antipourriel, antivirus, de détection d'intrusion et des pare-feu. De multiples programmes et versions logicielles sont utilisés pour protéger les courriels.

2.11 Applications de courrier électronique

De nos jours, les systèmes de courriel permettent l'intégration d'applications opérationnelles et administratives. Le nombre des applications est important, et elles comportent plusieurs niveaux d'intégration aux courriels.

Une première consultation auprès des partenaires de SPC a permis de constater qu'environ 2 250 applications étaient utilisées, soit des produits développés à l'interne et des produits commerciaux en vente libre, qui peuvent être intégrés à la solution de courriels regroupée. L'intégration de ces applications à un nouveau service de courrier électronique varie en complexité.

3. Utilisation de la messagerie électronique

3.1 Exemples de l'utilisation de la messagerie électronique

Exemples de courriels « internes » ordinaires qui comprennent des fonctions. Par exemple :

- Message, gestion des calendriers, planification;
- Avis (nouvelles et diffusion de renseignements);
- Collaboration (échange de renseignements);
- Approbations (absences, dépenses, charge de travail);
- Communications mobiles (par ex. BlackBerry[MD]).

Utilisation interne spéciale de courriel qui comprend les fonctions suivantes :

- Santé Canada – pour diffuser à l'interne de renseignements de sécurité sur des produits;
- Agence canadienne d'inspection des aliments (ACIA) – pour informer tous les inspecteurs qu'un produit alimentaire est rappelé;
- MAECI – pour envoyer des communications consulaires et diplomatiques.

1. Exemples de courriels externes comprenant les fonctions suivantes :

    - Messages à l'intention des citoyens – canadasite@canada.ca. Il s'agit d'un programme de RHDCC jumelé au numéro sans frais 1-800-OCanada, qui a pour but de répondre aux questions des citoyens;
    - RHDCC communique aussi avec les provinces concernant des ententes relatives au marché du travail;
    - La Direction générale des approvisionnements de TPSGC communique avec les entreprises canadiennes pour leur faire parvenir des demandes de propositions (DP) visant des services professionnels en informatique centrés sur les tâches (SPICT) et des services professionnels centrés sur les tâches et les solutions (SPTS), pour envoyer des contrats aux soumissionnairse et pour répondre aux questions des organisations;
    - Le Programme de sécurité industrielle (PSI) communique avec des représentants d'entreprises en ce qui a trait aux cotes de sécurité des membres de leur personnel;
    - L'ARC communique avec les entreprises et les citoyens canadiens afin de confirmer le statut de leurs transactions;
    - L'AFSC émet des alertes Amber, transmet des renseignements sur des opérations concernant les frontières, par exemple des renseignements sur des réfugiées transmis à d'autres ministères;
    - Le MDN utilise des adresses électroniques « anonymes » pour des raisons de sécurité;

- La GRC communique avec des organisations de police à l'étranger (par ex. Interpol);
- SC diffuse des messages sur des problèmes de santé publique et les solutions;
- Le MAECI communique avec la communauté diplomatique et les gouvernements étrangers;
- L'ACIA a recours à des courriels de protocole SMTP pour diffuser des alertes.

3.2 Situation géographique des utilisateurs

L'endroit à partir duquel les utilisateurs ont accès au système de courriel de SPC est un autre facteur important. Il existe plus de 1 000 points d'accès au Canada et à l'étranger, dont des centaines avec lecteurs de courriels.

ANNEXE D : DEMANDE ANTICIPÉE (PROVISOIRE) DE RÉPONSES POUR ÉVALUATION – PROCESSUS DE DÉTERMINATION DES RÉPONDANTS RETENUS

1 Introduction

Conformément à l'étape de demande de réponses pour évaluation (DRPE) de l'approche d'approvisionnement, le Canada doit préparer un document de DRPE. Selon les évaluations des répondants à cette demande, un sous-ensemble de répondants sera désigné par le Canada pour participer aux étapes subséquentes de l'examen et de la précision des exigences et de la demande de soumissions de l'approche d'approvisionnement.

La présente annexe renferme des critères techniques obligatoires et cotés qui serviront à choisir les répondants retenus à l'étape de la DRPE. La conformité à ces critères d'évaluation est essentielle pour fournir une solution de messagerie électronique conforme à la taille, à l'étendue et à la complexité de l'ITSC.

Ces exigences techniques obligatoires et cotées pourraient changer selon les commentaires de l'industrie.

Veuillez consulter la partie IV : Questions pour prendre connaissance des questions de l'industrie concernant les procédures proposées d'évaluation et de détermination des répondants retenus.

2 Procédures d'évaluation

Une équipe composée de représentants de SPC et de TPSGC évaluera les réponses des répondants à la DRPE. TPSGC et SPC pourront retenir les services d'un consultant indépendant, ou utiliser une ressource du GC pour évaluer les réponses. Chaque membre de l'équipe chargée de l'évaluation ne participera pas nécessairement à tous les aspects de l'évaluation.

Les répondants doivent satisfaire aux exigences techniques obligatoires et obtenir une note minimale pour les exigences techniques cotées pour être retenus et pouvoir participer à l'étape de l'examen et de la précision des exigences.

TPSGC a embauché un surveillant de l'équité dans le cadre de ce marché. Ce surveillant ne fera pas partie de l'équipe d'évaluation, mais il s'assurera que le Canada respecte la méthode d'évaluation décrite dans la demande de réponse pour évaluation.

3. Conditions pour la DRE et/ou la DDP

3.1 Sécurité

Le répondant doit satisfaire aux exigences de sécurité décrites dans la DDR.

3.2 Viabilité financière

Le répondant doit avoir la capacité financière nécessaire pour répondre à ce besoin. Afin de vérifier la capacité financière du soumissionnaire, TPSGC pourrait demander des renseignements financiers.

4. Exigences obligatoires en matière d'expérience technique de l'entreprise

Le Canada cherche des répondants qui possèdent une feuille de route éprouvée en conception, production et déploiement de solutions de courrier électronique, comme le décrit la partie III de la présente demande de renseignements.

Les répondants devront démontrer leur conformité à toutes les exigences obligatoires en matière d'expérience technique qui suivent, et fournir la documentation nécessaire pour l'appuyer.

Les exigences techniques obligatoires décrites ci-dessous seront évaluées selon la méthode « réussite ou échec » (p. ex. conforme ou non conforme). Les répondants qui ne satisfont pas aux exigences techniques obligatoires suivantes ne seront pas retenus.

4.1 Expérience de l'entreprise

Afin de satisfaire aux exigences techniques obligatoires liées à l'exigence O4, le répondant doit fournir une liste d'au moins 10 projets de transformation de services de courriels pour des organisations clientes réalisés au cours des cinq dernières années. Les renseignements requis sont :

(i) Le nom de l'entreprise;
(ii) Le nom et une courte description du projet;
(iii) Les dates et la durée du projet;
(iv) Le numéro de téléphone et l'adresse de courriel actuels de la personne-ressource de l'organisation cliente.

Afin de répondre aux exigences techniques obligatoires O1, O3, O4, O5 et O6, le répondant doit fournir des renseignements précis sur les travaux accomplis par son organisation, notamment des renseignements sur la plateforme de courriel utilisée, pour trois des dix projets précités. Un de ces projets devrait comprendre la mise en œuvre d'une solution de service de courriel sécuritaire, avec capacité de traitement des courriels secrets. La conformité aux exigences obligatoires O1 à O6 peut être démontrée à l'aide d'un ou de plusieurs des trois projets. Il n'est pas nécessaire que les projets soient les mêmes pour chaque exigence obligatoire (O1 à O6).

Le Canada pourrait faire des vérifications de validation de référence par écrit (par courriel) pour valider la véracité et l'exactitude des renseignements transmis par les répondants.

O1 : Le répondant doit avoir réalisé la conception, l'architecture, la production et la mise en œuvre de la solution de courrier électronique en tant que gestionnaire ou

fournisseur de services impartis pour un minimum de dix organisations clientes au cours des cinq dernières années.

O2: Le répondant doit actuellement fournir et gérer des services de courriels pour au moins dix organisations clientes avec :

(i) au moins 100 000 utilisateurs pour l'ensemble des organisations clientes;
(ii) au moins une organisation cliente regroupant au moins 50 000 utilisateurs;
(iii) au moins une organisation cliente au Canada regroupant au moins 25 000 utilisateurs.

O3: Le répondant doit avoir réalisé la conception, l'architecture, la production, la mise en œuvre et la gestion d'au moins une solution de courrier électronique sécuritaire pour un minium de 500 utilisateurs, avec capacité de traiter des courriels secrets, au cours des cinq dernières années.

O4: Le répondant doit fournir, depuis au moins 2 ans, des services de courriels disponibles en tout temps, 365 jours par année, pour au moins 3 organisations clientes, pour un total d'au moins 50 000 utilisateurs. Un centre d'aide bilingue (anglais et français) pour au moins une organisation cliente doit également être fourni. Ce centre doit être situé au Canada.

O5: Au cours des cinq dernières années, le répondant doit avoir réalisé la migration de systèmes de courrier électronique où la transformation touchait au moins 10 000 boîtes postales, sur une des plateformes de courriels suivantes **:**

(i) Microsoft Exchange;
(ii) Novell GroupWise; ou
(iii) IBM Lotus Notes Email.

O6: Au cours des cinq dernières années, le répondant doit avoir réalisé la conversion d'applications d'affaires intégrées à des systèmes de courrier électronique, où la transformation touchait au moins 10 000 boîtes postales, sur une des plateformes de courriels suivantes **:**

(i) Microsoft Exchange;
(ii) Novell GroupWise; ou
(iii) IBM Lotus Notes.

4. Exigences techniques cotées

Les répondants qui se conforment à toutes les exigences techniques obligatoires seront ensuite évalués et notés en fonction d'exigences techniques cotées (C1 à C6 décrites ci-dessous) selon l'expérience du répondant de la conception, de la production, du déploiement et de la gestion d'une solution de courriel d'entreprise, comme le décrit la DDR.

À cet égard, le Canada évaluera les répondants selon les exigences techniques cotées suivantes :

1. Expérience de l'entreprise
2. Exigences relatives aux services requis
3. Expérience en transformation de services de courriels

Chaque soumission de répondant sera évaluée selon les critères cotés (cotés dans la DRPE) ou selon une note de référence. Les répondants qui ne soumettront pas tous les renseignements demandés dans la DRPE seront notés en conséquence.

Critères	Exigences cotées	Maximum	Pondération
C1	Expérience de l'entreprise	600	40,0
C2	Exigences relatives aux services requis	100	10,0
C3	Expérience de la transformation de services de courriels	700	50,0
	Total	1400	100,0

Critères techniques cotés

Critères	Exigences cotées	Maximum	Pondé-ration
C1	**Expérience de l'entreprise**		**40 %**
C1.1	Le répondant doit indiquer le nombre d'organisations clientes à qui il fournit des services de courriels en tout temps, 365 jours par année (gestion comprise). Échelle de cotation 4 à 5 organisations clientes – 25 6 à 9 organisations clientes – 50 10 organisations clientes ou plus – 100	100	
C1.2	Le répondant doit fournir, pour les cinq dernières années, une feuille de route éprouvée de projets de conception, de production, de déploiement et de gestion de solutions de courriel dans un projet organisationnel complexe. Échelle de cotation 1 projet – 100 2 ou 3 projets – 150	200	

	Plus de 3 projets – 200		
C1.3	Le répondant doit fournir, pour les cinq dernières années, une feuille de route éprouvée de projets de conception, de production, de déploiement et de gestion de solutions de courriels devant respecter les processus législatifs et les politiques du gouvernement du Canada. Échelle de cotation 1 projet – 50 2 ou 3 projets – 75 Plus de 3 projets – 200	100	
C1.4	Le répondant doit fournir, pour les cinq dernières années, une feuille de route éprouvée de projets de conception, de production, de déploiement et d'opération d'une solution de courriels, pour un minimum de 500 utilisateurs, avec capacité de traitement de courriels secrets. Échelle de cotation 2 ou 3 projets – 150 Plus de 3 projets – 200	200	
C2	**Exigences relatives aux services requis**		**10 %**
C2.1	Le répondant doit fournir le nombre d'organisations clientes pour qui il fournit un centre d'aide bilingue (anglais et français) pour une solution de services de courriels. Échelle de cotation 2 ou 3 clients – 50 points Plus de 3 clients – 100 points	100	
C3.0	**Expérience de la transformation de services de courriels**		**50 %**
C3.1	Le répondant doit fournir le nombre de boîtes aux lettres d'organisations clientes dont il a assuré la migration. Échelle de cotation 10 000 à 99 999 boîtes aux lettres – 50 points 100 000 à 199 999 boîtes aux lettres : 75 points 200 000 boîtes aux lettres et plus – 100 points	100	
C3.2	Le répondant doit fournir, pour les cinq	200	

	dernières années, une feuille de route éprouvée de projets de gestion et de migration de systèmes de courriel, pour un minimum de 10,000 boîtes aux lettres, sur une des plateformes de courriel suivantes : i) Microsoft Exchange; ii) Novell GroupWise; iii) IBM Lotus Notes. Échelle de cotation 2 ou 3 projets – 100 Plus de 3 projets – 200		
C3.3	Le répondant doit fournir, pour les cinq dernières années, une feuille de route éprouvée de projets de gestion et de conversion d'applications opérationnelles, sur au moins une des plateformes de courriel suivantes : i) Microsoft Exchange; ii) Novell GroupWise; iii)IBM Lotus Notes. Échelle de cotation 2 ou 3 projets – 100 Plus de 3 projets – 200	200	
C3.4	Le répondant doit fournir, pour les cinq dernières années, une feuille de route éprouvée de projets de migration de l'intégralité des données, où il n'a causé la perte d'aucune donnée ni réduit les niveaux de service. Échelle de cotation : 1 projet – 75 2 – 3 projets – 150 Plus de 4 projets - 200	200	

5. Vérifications auprès des organisations clientes

Dans le cadre du processus de vérification pour la DRPE, des démarches pourraient être entreprises par courriel pour vérifier auprès des organisations clientes que les renseignements fournis par les répondants dans le Formulaire de vérification de projet de référence (à rédiger) sont véridiques et exacts.

6. Détermination des répondants retenus

Chaque répondant qui se conforme aux exigences techniques obligatoires et exigences techniques cotées sera retenu pour la détermination des meilleurs répondants et sera

invité à participer aux étapes de l’examen et de la précision des exigences et de la demande de soumissions de l’approche d’approvisionnement CPS.

La détermination de ces répondants sera fondée sur une méthode de sélection qui sera déterminée et décrite dans la DRPE.

ANNEXE E : MINISTÈRES ET ORGANISMES PARTENAIRES DE SPC

Affaires autochtones et Développement du Nord Canada (AADNC)
Affaires étrangères et Commerce international (MAECI)
Agence canadienne de développement économique du Nord (CanNor)
Agence canadienne de développement international (ACDI)
Agence canadienne d'inspection des aliments (ACIA)
Agence de développement économique du Canada pour les régions du Québec
Agence de la santé publique du Canada (ASPC)
Agence de promotion économique du Canada atlantique (APECA)
Agence des services frontaliers du Canada (ASFC)
Agence du revenu du Canada (ARC)
Agence fédérale de développement économique pour le Sud de l'Ontario (FedDev Ontario)
Agence spatiale canadienne (ASC)
Agriculture et Agroalimentaire Canada (AAC)
Anciens Combattants Canada (ACC)
Bibliothèque et Archives Canada (BAC)
Bureau du Conseil privé (BCP)
Centre d'analyse des opérations et déclarations financières du Canada (CANAFE)
Citoyenneté et Immigration Canada
Commission canadienne de sûreté nucléaire (CCSN)
Commission de la fonction publique du Canada (CFP)
Commission de l'immigration et du statut de réfugié du Canada (CISR)
Conseil national de recherches du Canada (CNRC)
Diversification de l'économie de l'Ouest Canada (DEO)
École de la fonction publique du Canada (EFPC)
Environnement Canada (EC)
Gendarmerie royale du Canada (GRC)
Industrie Canada (IC)
Infrastructure Canada (INFC)
Ministère de la Défense nationale (MDN)
Ministère de la Justice (JUS)
Ministère des Finances
Parcs Canada (PC)
Patrimoine canadien (PCH)
Pêches et Océans Canada (MPO)
Ressources humaines et Développement des compétences Canada (RHDCC)
Ressources naturelles Canada (RNCan)
Santé Canada (SC)
Secrétariat du Conseil du Trésor du Canada (SCT)
Sécurité publique Canada (SP)
Service correctionnel du Canada (CIC)

Statistique Canada (StatCan)
Transports Canada (TC)
Travaux publics et Services gouvernementaux Canada (TPSGC)

ANNEXE F : LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

Le document qui suit est la liste de vérification des exigences relatives à la sécurité (LVERS). Pour visualiser le formulaire, double-cliquez sur l'objet ci-dessous

"LVERS ebauche.pdf"

Objet 1 LVERS ebauche

ANNEXE G : INSTURMENTS LÉGISLATIFS ET INSTRUMENTS DE POLITIQUE DU SECRÉTARIAT DU CONSEIL DU TRÉSOR

Les instruments de politiques mentionnés ci-dessous pourraient avoir un effet sur l'Initiative de transformation des services de courriels. Cette liste fait actuellement l'objet d'un examen et pourrait être modifiée.

1 POLITIQUES

Politique sur la sécurité du gouvernement
Politique sur les services communs
Politique sur l'accès à l'information
Politique sur la protection de la vie privée
Politique de communication
Politique sur les marchés
Cadre de politique sur la gestion des actifs et services acquis
Politique sur la gestion de la TI
Cadre de politiques en matière de langues officielles
Politique sur l'obligation de prendre des mesures d'adaptation pour les personnes handicapées dans la fonction publique fédérale
Politique de gestion des projets
Politique d'utilisation des réseaux électroniques
Politique relative à la gestion de l'information

2. Directives

Directive sur la gestion de l'identité
Directive sur la gestion des technologies de l'information
Directive sur la tenue de documents

3. Normes et lignes directrices

Gestion de la sécurité des technologies de l'information
Norme pour les systèmes de gestion électronique des documents et des dossiers
Norme sur les métadonnées
Normes sur l'accessibilité et la facilité d'emploi des sites Web
NCTTI 26 : Évaluation de logiciels – Caractéristiques de la qualité d'un logiciel et directives d'utilisation
NCTTI 3 : Jeu de caractères codés pour les échanges d'information
NCTTI 36 : Représentation numérique de la date et de l'heure
NCTTI 6,9 : Critères des applications des systèmes ouverts au Canada (CASOC), Réseau de câblage de télécommunications des immeubles dont l'État est propriétaire ou locataire

ANNEXE H : **ENTENTE DE NON-DIVULGATION**

ENTENTE RÉCIPROQUE
DE NON-DIVULGATION
entre

_____

et
SA MAJESTÉ LA REINE DU CHEF DU CANADA
représentée par
LE MINISTRE DE LA DÉFENSE NATIONALE
au nom du
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA

Nature de l'entente

1. Le présent document est une entente de non-divulgation entre _____ (la « société »), une personne morale constituée en vertu des lois de _____ et dont les bureaux principaux sont situés au _____ :
et le Centre de la sécurité des télécommunications Canada (« CSTC »), qui a des bureaux au 719, chemin Héron, Ottawa, ON, K1G 3Z4.

Objectif de l'entente

2. L'objectif de la présente entente est de permettre au CSTC de fournir des renseignements de nature délicate sur les menaces à l'approvisionnement, en vue de l'élaboration des stratégies d'atténuation des risques pour les fournisseurs de solutions de courriel de l'Initiative de transformation des services de courriels (solution d'ITSC pour le gouvernement du Canada [GC]), et de permettre au CSTC de recevoir des renseignements de nature exclusive de la société ou des renseignements qui ne doivent pas être divulgués à ses concurrents.

Définition

L'expression « renseignements de nature délicate », lorsqu'il est question d'information, signifie des renseignements désignés ou classés par l'État comme étant TRÈS SECRETS, SECRETS, CONFIDENTIELS OU PROTÉGÉS.

Conditions de l'entente

3. Compte tenu de l'échange réciproque de renseignements ainsi que des engagements réciproques que comporte la présente entente, la société et le CSTC conviennent de ce qui suit :

Renseignements de nature exclusive de la société

4.

(a) Chaque fois que la société divulgue au CSTC des renseignements qu'elle considère comme étant de nature exclusive ou comme ne devant pas être divulgués aux concurrents, la société doit sur-le-champ l'indiquer clairement, par écrit, avec la mention « Renseignements de nature exclusive »;

(b) Si une telle divulgation a lieu verbalement ou visuellement, les renseignements verbaux ou visuels doivent être présentés au moment de leur divulgation comme étant des renseignements de nature exclusive. La société doit consigner par écrit, sans délai, le fait qu'il s'agit de renseignements de nature exclusive.

5. Le CSTC doit maintenir la confidentialité des renseignements désignés comme étant de nature exclusive lorsqu'il communique avec d'autres organismes gouvernementaux et il ne doit utiliser ces renseignements qu'en lien avec l'objectif énoncé ci-dessus.

6. Les parties reconnaissent que la présente entente de non-divulgation est assujettie à la *Loi sur l'accès à l'information* (L.R.C. (1985), ch. A-1, modifié) et que les demandes d'accès à l'information assujettie à la présente entente de non-divulgation seront régies par les dispositions de cette *loi*.

7. Les renseignements de nature exclusive ne bénéficieront pas de la protection prévue à la présente entente s'ils :

(a) ont été produits par le CSTC de façon indépendante ou sont déjà connus du CSTC au moment de leur divulgation;

(b) sont connus du CSTC ou accessibles à celui-ci par l'intermédiaire d'une autre source que la société, sans violation de la présente entente de la part du CSTC;

(c) ont été rendus accessibles au public;

(d) ont été publiés pour quiconque sans restriction par la société.

8. Tous les renseignements de nature exclusive doivent demeurer la propriété de la société et lui être retournés ou être détruits, selon le choix de la société, dans les 30 jours suivant une demande à cet égard de cette dernière.

Renseignements de nature délicate du CSTC

9.

(a) Chaque fois que le CSTC divulgue à la société des renseignements qu'il considère comme étant de nature délicate, il doit l'indiquer clairement, par écrit, avec la mention « Renseignements de nature délicate »;

(b) Si une telle divulgation a lieu verbalement ou visuellement, les renseignements verbaux ou visuels doivent être présentés au moment de leur divulgation comme étant des renseignements de nature délicate. Le CSTC doit consigner par écrit, sans délai, le fait qu'il s'agit de renseignements de nature exclusive.

10. La société doit maintenir la confidentialité des renseignements désignés comme étant de nature délicate. Sans consentement écrit préalable du CSTC, la société ne doit permettre à personne d'accéder à des renseignements de nature délicate à moins qu'il ne s'agisse d'un employé de la société disposant d'une attestation de sécurité qui correspond au niveau de confidentialité des renseignements de nature délicate consultés. La société doit aviser sur-le-champ le CSTC si une personne accède à des renseignements de nature délicate sans disposer de l'attestation de sécurité appropriée.

11. Tous les renseignements de nature délicate doivent demeurer la propriété du CSTC et lui être retournés ou être détruits, selon le choix du CSTC, dans les 30 jours suivant une demande à cet égard de ce dernier.

12. La présente entente est régie, analysée et interprétée conformément aux lois de la province de l'Ontario (Canada).

13. La présente entente entrera en vigueur une fois qu'elle aura été signée par les deux parties et le demeurera pendant _____ ans, à moins qu'elle ne soit résiliée plus tôt par écrit, avec la signature des deux parties.

14. La présente entente ne peut être modifiée que par écrit, avec la signature des deux parties.

_____	_____
Nom de la société télécommunications	Centre de la sécurité des Canada
_____	_____
Signature	Signature
_____	_____
Titre	Titre
_____	_____
Date	Date

ANNEXE I : FORMULAIRE D'INSCRIPTION À UNE **SÉANCE D'INFORMATION DU CSTC** SUR LES MENACES À L'APPROVISIONNEMENT

Formulaire d'inscription à une séance d'information les menaces à l'approvisionnement

Remarque : Le Canada déterminera la date et l'heure de ces séances d'information. Au plus tard le 3 juillet 2012, à 16 h (HAE), il en informera par courriel toutes les parties qui auront soumis le présent formulaire.

Quel est le nom de votre entreprise ou de votre association?

Nom : _____

Veuillez indiquer le ou les emplacements où vos représentants assisteront à l'atelier ainsi que le nom des représentants :

Emplacement	Nom des représentants	Emplacement	Nom des représentants
Calgary		Région de la capitale nationale	
Edmonton		Toronto	
Halifax		Vancouver	

Montreal		Winnipeg	

Veuillez fournir une adresse de courriel que TPSGC peut utiliser pour vous répondre et confirmer la date, l'heure ainsi que l'adresse ou l'emplacement de la salle :

Adresse de courriel : _____

ANNEXE J : FORMULAIRE D'INSCRIPTION À UN ATELIER SUR LES DEMANDES DE RENSEIGNEMENTS (DDR)

Formulaire d'inscription à un atelier sur les DDR

Remarque : Le Canada déterminera l'adresse ou l'emplacement de la salle des ateliers. Au plus tard le 6 juillet 2012, à 16 h HAE, il en informera toutes les parties qui auront soumis le présent formulaire.

Quel est le nom de votre entreprise ou de votre association?

Nom : _____

Veuillez indiquer le ou les emplacements où vos représentants assisteront à l'atelier ainsi que le nom des représentants :

Emplacement	Nom des représentants	Emplacement	Nom des représentants
Calgary		Région de la capitale nationale	
Edmonton		Toronto	
Halifax		Vancouver	

Montreal		Winnipeg	

Veuillez fournir une adresse de courriel que TPSGC peut utiliser pour vous répondre et confirmer l'adresse ou l'emplacement de la salle :

Adresse de courriel : _____