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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution

Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Title - Sujet National Cybercrime Solution Projec Solution nationale en matière de cybercriminalité	
Solicitation No. - N° de l'invitation M7594-205915/D	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client M7594-205915	**Date** 2021-04-12
GETS Reference No. - N° de référence de SEAG PW-$$XL-155-39352	
File No. - N° de dossier 155xl.M7594-205915	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-05-25 Heure Avancée de l'Est HAE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Labossière, Jean-Claude	**Buyer Id - Id de l'acheteur** 155xl
Telephone No. - N° de téléphone (613) 858-7359 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

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

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

Ce document d'appel d'offres final annule et remplace intégralement le document d'appel d'offres antérieurement affiché.

DEMANDE DE PROPOSITIONS

SOLUTION NATIONALE EN MATIERE DE CYBERCRIMINALITE (SNC)

POUR

GENDARMERIE ROYALE DU CANADA (GRC)

Table des matières

DEMANDE DE PROPOSITIONS

SOLUTION NATIONALE EN MATIÈRE DE CYBERCRIMINALITÉ (SNC)

POUR LA

GENDARMERIE ROYALE DU CANADA (GRC)

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La demande de soumissions contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

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

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

Partie 3 Instructions pour la préparation des soumissions : donne aux soumissionnaires des instructions sur la façon de préparer leur soumission;

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

Partie 5 Attestations et autres renseignements : renferme une description de toutes les attestations et des autres renseignements à fournir;

Partie 6 Exigences relatives à la sécurité, exigences financières et autres exigences : décrit les exigences particulières auxquelles les soumissionnaires doivent répondre;

Partie 7 Clauses du contrat subséquent : contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

Les annexes comprennent, notamment, l'énoncé des travaux.

1.2 Résumé

a) Une demande de renseignements (DDR) (M7594-200151/A) a été émise le 5 juin 2019. La consultation de l'industrie avait pour objectif principal de solliciter ses commentaires sur les exigences générales du Canada afin de déterminer l'intérêt et la capacité de l'industrie à fournir la solution proposée.

b) Des avis de projet de marché (APM) M7594-205915/A, M7594-205915/B et M7594-205915/C ont été publiés respectivement le 22 mai 2020, le 3 décembre 2020 et le 28 janvier 2021 afin de consulter davantage l'industrie et obtenir ses commentaires sur l'ébauche des exigences

et l'approche d'approvisionnement du Canada afin de permettre au Canada de mieux définir ses exigences et son approche d'approvisionnement.

c) La présente demande de soumissions (propositions) vise à acquérir la Solution nationale en matière de cybercriminalité (SNC) (la « solution »). Cependant, la présente demande de soumissions permettra aussi au Canada de mettre la solution à la disposition de tous les ministères et de toutes les sociétés d'État (selon la définition de ces termes dans la Loi sur la gestion des finances publiques) ou encore de toute autre partie pour le compte de laquelle TPSGC est autorisé à agir, à l'occasion, en vertu de l'article 16 de la Loi sur le ministère des Travaux publics et des Services gouvernementaux (chaque partie étant un « client »). Bien que le Canada puisse mettre la solution logicielle à la disposition de l'ensemble des clients, cette demande de soumissions n'empêche nullement l'application par le Canada d'une autre méthode d'approvisionnement pour toute autre entité du gouvernement du Canada ayant des besoins similaires.

d) La demande de propositions (DP) vise à attribuer un maximum de trois contrats aux soumissionnaires retenus pour les travaux de la phase 1 afin que chacun d'eux développe un prototype de solution pour une évaluation des capacités et de la convivialité (ECC) conformément à la phase 1 de l'annexe A – Énoncé des travaux. À l'issue des travaux de la phase 1 et après l'évaluation des prototypes de solution par le Canada et la réalisation réussie d'un test de prototype sur plateforme par un entrepreneur (s'il y a lieu), le Canada exercera, à sa seule discrétion, l'option en faveur de l'entrepreneur pour la livraison de la solution complète conformément à la phase 2 de l'annexe A – Énoncé des travaux. À la suite des travaux de la phase 2 relatifs à la mise en œuvre de la solution complète, le Canada exercera au besoin, et à sa seule discrétion, les huit périodes d'option irrévocables d'un an chacune pour prolonger au besoin la durée du contrat.

e) Bien que le Canada ait l'intention d'établir des contrats d'une durée déterminée, il se réserve le droit de continuer à conclure des contrats pour ces solutions et d'en tirer parti aussi longtemps qu'il le juge logique sur le plan commercial. Le Canada s'attend également à ce que ce type de solution évolue avec le temps et la technologie, y compris l'intégration de fonctionnalités ou de technologies qui ne fait pas partie des exigences actuelles. Le Canada se réserve le droit d'envisager l'inclusion de ces fonctionnalités ou technologies évolutives dans la portée continue des travaux effectués en vertu des contrats, sous réserve des processus d'approbation internes du Canada. Le Canada se réserve le droit, à une date ultérieure et à sa seule discrétion, de définir la solution comme étant une solution multi ministérielle ou de désigner la solution comme étant une solution normalisée à l'échelle du gouvernement du Canada, si et quand le Comité d'examen de l'architecture d'entreprise du gouvernement du Canada (CEAEGC) le détermine.

f) Le client est à la recherche d'une solution offerte au moyen d'un modèle de prestation de services d'informatique en nuage qui peut comprendre n'importe quelle combinaison de logiciels hébergés par la Gendarmerie royale du Canada (GRC), sur l'infrastructure locataire Protégé B en tant que service (IaaS) de la GRC, sur une plateforme privée en tant que service (PaaS), sur une plateforme publique en tant que service (PaaS) et sur un logiciel en tant que service (SaaS) utilisant une plateforme de service d'informatique en nuage Protégé B approuvée par le gouvernement du Canada. La solution requise pourrait comprendre n'importe quelle combinaison de logiciels commerciaux (COTS) libres ou personnalisés; la configuration subséquente de ces logiciels doit permettre l'exploitation de la solution en tout temps, conformément à l'Annexe A – Énoncé des travaux. L'entrepreneur doit définir un modèle de prestation des services d'informatique en nuage compatible avec les exigences de sécurité Protégé B des services d'informatique en nuage du gouvernement du Canada (GC).

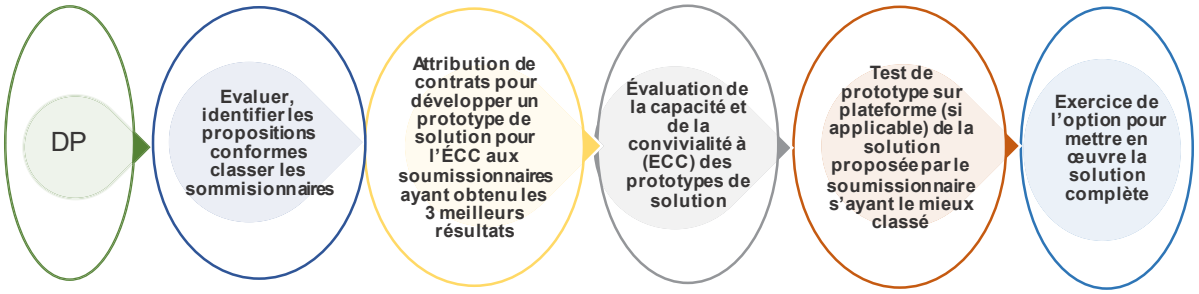
g) La portée des travaux pour la solution prototype de l'ACU comprend la planification, la conception, l'élaboration, la configuration, la mise à l'essai et l'exécution d'une solution de produit minimum viable (PMV) hébergée, de qualité de production et fonctionnant en nuage

qui prend en charge jusqu'à cent (100) utilisateurs, conformément aux exigences techniques et fonctionnelles décrites à l'Annexe A – Énoncé des travaux.

h) La portée des travaux pour la solution complète comprend la planification, la conception, l'élaboration, la configuration, la documentation, la mise à l'essai et le déploiement de toutes les capacités fonctionnelles et non fonctionnelles décrites à l'Annexe C – Modèle de capacité opérationnelle du SNC de l'Annexe A – Énoncé des travaux. La solution doit prendre en charge jusqu'à 2 000 utilisateurs, dont 500 simultanément, et être en mesure de prendre en charge les processus et les activités d'analyse qui devraient permettre d'accumuler 110 To de données par année. Voir l'Annexe A – Énoncé des travaux, pour connaître tous les détails.

i) La demande de propositions et le(s) contrat(s) subséquent(s) suivront une approche d'approvisionnement souple selon une évaluation en deux étapes afin d'encourager une collaboration plus efficace avec les fournisseurs. Par « souplesse », on entend le fait d'aborder les projets par petites étapes mais à un rythme rapide, tout en évaluant et en réglant les problèmes en cours de route.

j) Le processus d'approvisionnement souple prévu se déroulera selon les phases suivantes :



1.3 Aperçu du projet

a) Le Gouvernement du Canada est à la recherche d'une solution logicielle qui sera déployée chez un locataire de solution infonuagique rencontrant la norme de sécurité Protégé B, Intégrité moyenne, Disponibilité moyenne (PBMM). La solution requise pourrait comprendre n'importe quelle combinaison de logiciels commerciaux (COTS), en source ouverte, ou sur mesure; la configuration subséquente d'un tel logiciel doit permettre l'exploitation de la solution en tout temps conformément à l'Énoncé des travaux. L'entrepreneur devra configurer la solution de manière à ce :

(i) qu'elle respecte les exigences relatives à la sécurité du gouvernement du Canada et les pratiques exemplaires de l'industrie;
(ii) qu'elle comprenne de la maintenance et du soutien technique sécurisés;
(iii) qu'elle comprenne la formation et d'autres services professionnels sur demande; et
(iv) qu'elle comprenne des documents de formation en français et en anglais régulièrement mis à jour et de la documentation sur les solutions, y compris toutes les licences de logiciel et les garanties requises.

Le gouvernement du Canada conservera la propriété de toutes les données de la solution, y compris les données opérationnelles, les données de surveillance et les métadonnées.

b) Le besoin est assujetti aux dispositions de l'Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP-OMC), de l'Accord de libre-échange Canada-Chili (ALECCH),

de l'Accord de libre-échange Canada Colombie (ALECCO), de l'Accord de libre-échange Canada-Panama (ALECPA), l'Accord économique et commercial global (AECG) entre le Canada et l'Union européenne, s'il est en vigueur, de l'Accord de libre-échange Canada Corée (ALECC), de l'Accord de libre-échange Canada Pérou (ALECP), de l'Accord de libre-échange Canada Ukraine (ALECK) et de l'Accord de partenariat transpacifique global et progressiste (PTPGP).

c) La demande de propositions permettra aux soumissionnaires d'utiliser le service Connexion postel offert par la Société canadienne des postes pour présenter leur soumission par voie électronique. Les soumissionnaires doivent consulter la partie 2 intitulée « Instructions à l'intention des soumissionnaires » et la partie 3 intitulée « Instructions pour la préparation des soumissions » de la demande de soumissions, pour de plus amples renseignements.

d) Le Programme de contrats fédéraux pour l'équité en matière d'emploi s'applique au présent besoin (voir la partie 5, Attestations et renseignements supplémentaires, la partie 7, Clauses du contrat subséquent, et le formulaire intitulé Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation).

Aperçu de l'approche de l'approvisionnement souple

Le processus d'approvisionnement sera mené selon une approche souple comme suit :

1. **Appel d'offres (Phase 1):** Cette demande de propositions finale est émise par l'entremise du Service électronique d'appels d'offres du gouvernement pour une période définie afin de satisfaire aux exigences du **client**. Les soumissionnaires ont l'occasion d'examiner le document d'appel d'offres, de demander des précisions sur tout aspect du document d'appel d'offres et de présenter une soumission en réponse à l'appel d'offres.

2. **Évaluer les propositions pour déterminer et classer les soumissionnaires recevables (Phase 2)**: Les soumissions seront évaluées conformément à toutes les exigences de la demande de soumissions. Les soumissions seront évaluées en fonction des critères d'évaluation technique et financière énoncés dans la demande de soumissions. Les soumissionnaires qui satisfont à toutes les exigences obligatoires de la demande de soumissions seront classés en fonction de la cote combinée la plus élevée des évaluations techniques et financières. Le processus d'évaluation détaillé est décrit à la partie 4 – Évaluation et évaluation.

3. **Attribuer des contrats à un maximum de trois soumissionnaires les mieux classés pour fournir un prototype de solution (Phase 3)**: Sur la base des résultats de l'évaluation technique et financière, le Canada peut attribuer jusqu'à trois contrats d'une valeur initiale de 200 000 $ (TPS/TVH en sus) aux trois soumissionnaires les mieux classés pour développer et livrer un prototype de solution dans un délai déterminé, conformément aux travaux de la phase 1 décrits à l'annexe A – Énoncé des travaux et aux critères de l'évaluation des capacités et de la convivialité (ECC) de l'appendice A de l'annexe A – Énoncé des travaux.

4. **Effectuer une évaluation de la capacité et de la convivialité (ÉCC) (Phase 4)**: À la suite de l'achèvement et de la livraison de tous les produits livrables requis, y compris le prototype de solution pour les travaux de la phase 1 de l'annexe A – Énoncé des travaux, le Canada procédera à une évaluation de la capacité et de la convivialité du prototype conformément aux critères de l'ÉCC énoncés à l'annexe A – Énoncé des travaux. Le processus d'évaluation détaillé de l'ÉCC est décrit à la partie 4 – Procédures d'évaluation et de sélection.

5. **Réalisation du test de prototype sur plateforme de la solution la mieux classée après l'ECC, dans l'écosystème de la GRC (Phase 5)**: Après la réalisation de l'ECC, les entrepreneurs seront classés en fonction de la meilleure note combinée de leurs résultats techniques, financiers et d'ECC. Un test de prototype sur plateforme peut être effectué, à la seule discrétion du Canada, de la solution proposée par l'entrepreneur le mieux classé

(identifié après l'ECC) pour valider les exigences techniques et fonctionnelles. Le processus détaillé de test de prototype sur plateforme est décrit à la Partie 4 – Procédures d'évaluation et méthode de sélection.

6. **Exercer l'option pour mettre en œuvre la Solution complète (Phase 6)**: Le Canada exercera, à sa seule discrétion, son option irrévocable en faveur de l'entrepreneur le mieux classé dont la solution prototype a été validée par rapport aux exigences techniques et fonctionnelles du SNC. L'exercice de cette option lancera la mise en œuvre de la solution complète conformément aux travaux de la phase 2 décrits à l'annexe A - Énoncé des travaux. Le Canada a l'intention d'exercer son option irrévocable auprès de l'entrepreneur le mieux classé pour mettre en œuvre la solution complète. Toutefois, le Canada peut, à sa seule discrétion, exercer son option irrévocable sur les autres contrats pour une partie des travaux décrits pour la phase 2 de l'annexe A-Énoncé des travaux s'il est déterminé que cela répondrait le mieux aux besoins du Canada.

1.4 Exigences relatives à la sécurité

a) Le présent besoin comporte des exigences relatives à la sécurité. Des exigences de sécurité différentes s'appliqueront à chacun des travaux de la phase 1 et de la phase 2 décrits dans l'annexe A – Énoncé des travaux. Avant d'attribuer un contrat pour la phase 1, et avant de prolonger un contrat pour la phase 2, les conditions suivantes doivent être remplies:

(i) le soumissionnaire (ou l'entrepreneur) doit détenir une attestation de sécurité d'organisme valable tel qu'il est indiqué à la partie 6 – Clauses du contrat subséquent;

(ii) les personnes proposées par le soumissionnaire (ou l'entrepreneur) et qui doivent avoir accès à des renseignements ou à des biens de nature protégée ou classifiée ou à des lieux de travail dont l'accès est réglementé doivent posséder une attestation de sécurité telle qu'il est indiqué à la partie 6 – Clauses du contrat subséquent;

(iii) le soumissionnaire (ou l'entrepreneur) doit fournir le nom de toutes les personnes qui devront avoir accès à des renseignements ou à des biens classifiés ou protégés, ou encore à des établissements de travail dont l'accès est réglementé;

(iv) le lieu proposé par le soumissionnaire (ou l'entrepreneur) pour la réalisation des travaux et la sauvegarde des documents doit satisfaire aux exigences relatives à la sécurité précisées à la Partie 6 – Clauses du contrat subséquent; et

(v) le soumissionnaire doit fournir les adresses des emplacements ou des locaux proposés pour l'exécution des travaux et les documenter, tout en assurant la protection indiquée à la Partie 3 – Section IV Renseignements supplémentaires.

b) On rappelle au soumissionnaire (ou à l'entrepreneur) qu'il doit obtenir la cote de sécurité requise dans les plus brefs délais. La décision de retarder l'attribution du contrat (ou l'autorisation d'exécuter le travail) pour permettre au soumissionnaire (ou à l'entrepreneur) retenu d'obtenir la cote de sécurité nécessaire demeure à l'entière discrétion de l'autorité contractante.

c) Pour obtenir de plus amples renseignements sur les exigences relatives à la sécurité, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

1.5 Comptes rendus

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

1.6 Conflit d'intérêts – Avantage indu

a) Afin de protéger l'intégrité du processus d'approvisionnement, les soumissionnaires sont avisés que le Canada peut rejeter une soumission dans les circonstances suivantes :

(i) le soumissionnaire, un de ses sous-traitants, un de leurs employés respectifs, actuels ou anciens, a participé d'une manière ou d'une autre à la préparation de la demande de soumissions ou est en situation de conflit d'intérêts ou d'apparence de conflit d'intérêts;

(ii) le Canada juge que le soumissionnaire, un de ses sous-traitants, un de leurs employés respectifs, actuels ou anciens, a eu accès à des renseignements relatifs à la demande de soumissions qui n'étaient pas à la disposition des autres soumissionnaires et que cela donne ou semble donner au soumissionnaire un avantage indu.

b) Le Canada ne considère pas, qu'en soit, l'expérience acquise par un soumissionnaire qui fournit ou a fourni les biens et services décrits dans la demande de soumissions (ou des biens et des services similaires) représente un avantage indu en faveur du soumissionnaire ou crée un conflit d'intérêts. Le soumissionnaire demeure cependant assujetti aux critères énoncés ci-dessus.

c) Dans le cas où le Canada a l'intention de rejeter une soumission conformément au présent article, l'autorité contractante en informera le soumissionnaire et lui donnera la possibilité de faire valoir son point de vue, avant de prendre une décision définitive. Les soumissionnaires ayant un doute par rapport à une situation particulière devraient communiquer avec l'autorité contractante avant la date de clôture de la demande de soumissions. En déposant une soumission, le soumissionnaire déclare qu'il n'est pas en conflit d'intérêts et qu'il ne bénéficie d'aucun avantage indu. Le soumissionnaire reconnaît que le Canada est seul habilité à établir s'il existe un conflit d'intérêts, un avantage indu ou une apparence de conflit d'intérêts ou d'avantage indu.

d) Sans limiter d'aucune façon les dispositions décrites au paragraphe 1.6(a) ci-dessus, les soumissionnaires sont priés de noter que le Canada a fait appel aux entrepreneurs et aux ressources ci-dessous du secteur privé qui ont assuré la prestation de certains services, notamment l'examen du contenu pour la préparation de la présente demande de soumissions, et/ou qui ont eu ou pourraient avoir eu accès aux renseignements relatifs au contenu de la demande de soumissions ou à d'autres documents ayant trait à cette demande de soumissions:

ADGA Group Consultants Inc.
- Joe Carlucci
- Gardy Joseph

Cache Computer Consulting Corp
- Todd Mennie

Cofomo Ottawa (formerly operating as: Emerion)
- Ying Chen
- John Zhang

Experis-Veritaaq
- Justin Richardson
- Kevin Yang
- David Dang

Gartner, Inc.
- Chris Litton
- Alasdair Maughan
- Corry Robinson

Info-Tech Research Group
- Alex Ciraco

MODIS
- Joan Duval
- Patrick Quinlan
- Deborah Rudd
- Alex Aronec

S.i. Systems ULC
- Warren Chen
- Richard Legault
- Brad Martel
- Rob Webb
- Scott Webster
- Andrew Taylor

The Powell Group-TPG Technology Consulting Ltd
- Stephen Archdeacon

e) Toute soumission reçue de l'un des entrepreneurs susmentionnés en vertu de l'alinéa 1.6(d), qu'il s'agisse d'un soumissionnaire unique, d'une coentreprise ou d'un sous-traitant d'un soumissionnaire, pour laquelle l'une des ressources susmentionnées a contribué à la soumission, sera considérée comme contrevenant aux clauses sur les conflits d'intérêts énoncées dans la présente section, et la soumission sera déclarée non recevable.

1.7 Processus de conformité des soumissions par étapes

Le processus de conformité des soumissions par étapes s'applique à ce besoin.

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions uniformisées, clauses et conditions

a) Toutes les instructions, clauses et conditions précisées dans la demande de soumissions par numéro, par date et par titre sont reproduites dans le *Guide des clauses et conditions uniformisées d'achat* publié par Services publics et Approvisionnement Canada (SPAC).

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

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

d) Le paragraphe 5(4) du document 2003, Instructions uniformisées – biens ou services – besoins concurrentiels est modifié de la façon qui suit :

(i) Supprimer : 60 jours

(ii) Insérer : 180 jours

e) Les instructions uniformisées 2003 sont modifiées comme suit :

1. L'article 5, Présentation des soumissions, est modifié comme suit :
   i. Le paragraphe 1 est entièrement supprimé et remplacé par ce qui suit : « Le Canada exige que chaque soumission, à la date et à l'heure de clôture de la demande ou sur demande de l'autorité contractante, par exemple dans le cas d'une soumission acheminée par Connexion postel, soit signée par le soumissionnaire ou par son représentant autorisé. Si une soumission est présentée par une coentreprise, elle doit être conforme à l'article intitulé Coentreprise. »
   ii. Le paragraphe 2d. est entièrement supprimé et remplacé par ce qui suit : « de faire parvenir sa soumission uniquement au Module de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) indiqué dans la demande de soumissions ou à l'adresse indiquée dans la demande de soumissions, selon le cas ».
   iii. Le paragraphe 2e. est entièrement supprimé et remplacé par ce qui suit : « de veiller à ce que le nom, l'adresse de l'expéditeur et le numéro d'entreprise pour l'approvisionnement, le numéro de la demande de soumissions ainsi que la date et l'heure de clôture de la demande soient clairement indiqués dans la soumission ».
2. L'article 06, soumissions déposées en retard, est entièrement supprimé et remplacé par le suivant : « TPSGC renverra les soumissions livrées après la date et l'heure de clôture stipulées dans la demande de soumissions, à moins que ces soumissions ne soient considérées comme des soumissions retardées selon les circonstances énoncées à l'article intitulé Soumissions retardées. Les soumissions transmises par un moyen autre que le service Connexion postel de la Société canadienne des postes seront renvoyées. Dans le cas des soumissions transmises à l'aide du service Connexion postel, les conversations entamées par le Module de réception des soumissions à l'aide du service Connexion postel qui comportent un accès, des dossiers et des renseignements relatifs à une soumission déposée en retard seront supprimées. »
3. L'article 7, Soumissions retardées, est modifié comme suit :
   i. Le paragraphe 1 est modifié pour ajouter l'élément de preuve suivant « d. une date et heure de l'envoi du service Connexion postel de la SCP indiquée dans l'activité de la conversation du service Connexion postel. »

4. L'article 8, Transmission par télécopieur, est supprimé et remplacé par ce qui suit : « par Connexion postel »

2.2 Soumission des offres

a) Les soumissions doivent seulement être présentées à l'Unité de réception des soumissions de Services publics et Approvisionnement Canada (SPAC) au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions, à l'aide du service Connexion postel, à l'adresse électronique suivante : tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca .

b) En raison de la nature de l'appel d'offres, les soumissions transmises par télécopieur à SPAC ne seront pas acceptées.

2.3 Ancien fonctionnaire

Les contrats attribués à d'anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen public le plus minutieux et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats attribués à d'anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous avant l'attribution du contrat. Si la réponse aux questions et, s'il y a lieu, les renseignements requis n'ont pas été fournis à la date de la fin de l'évaluation des soumissions, le Canada informera le soumissionnaire du délai qui lui est imparti pour fournir l'information. Le défaut de réponse à la demande du Canada et le défaut de conformité avec les exigences dans les délais prévus entraîneront l'irrecevabilité de la soumission.

Définitions

Aux fins de cette clause, « ancien fonctionnaire » signifie tout ancien employé d'un ministère au sens de la *Loi sur la gestion des finances publiques*, L.R., 1985, ch. F-11, un ancien membre des Forces armées canadiennes ou de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :

a) une personne;

b) une personne qui s'est constituée en personne morale;

c) une société de personnes constituée d'anciens fonctionnaires; ou

d) une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

« période du paiement forfaitaire » signifie la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou vers un autre emploi par suite de la mise en place des divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l'allocation de fin de services, qui se mesure de façon similaire.

« pension » signifie une pension ou une allocation annuelle versée en vertu de la *Loi sur la pension de la fonction publique* (LPFP), L.R., 1985, ch. P-36, et toute augmentation versée en vertu de la *Loi sur les prestations de retraite supplémentaires*, L.R., 1985, ch. S-24, dans la mesure où elle touche la LPFP. La pension ne comprend pas les pensions payables conformément à la *Loi sur la pension de retraite des Forces canadiennes*, L.R., 1985, ch. C-17, à la *Loi sur la continuation de la pension des services de défense*, 1970, ch. D-3, à la *Loi sur la continuation des pensions de la Gendarmerie royale du Canada*, 1970, ch. R-10, et à la Loi sur la pension de retraite de la

Gendarmerie royale du Canada, L.R., 1985, ch. R-11, à la *Loi sur les allocations de retraite des parlementaires*, L.R., 1985, ch. M-5, et à la partie de la pension versée conformément à la *Loi sur le Régime de pensions du Canada*, L.R., 1985, ch. C-8.

Ancien fonctionnaire touchant une pension

Selon les définitions ci-dessus, est-ce que le soumissionnaire est un ancien fonctionnaire touchant une pension? **Oui** ( ) **Non** ( )

Si oui, le soumissionnaire doit fournir l'information suivante pour tous les anciens fonctionnaires touchant une pension, le cas échéant :

a) le nom de l'ancien fonctionnaire;

b) la date de cessation d'emploi dans la fonction publique ou de la retraite.

En fournissant cette information, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension, soit publié dans les rapports de divulgation proactive des marchés, sur les sites Web des ministères, et ce conformément à l'Avis sur la Politique des marchés : 2012-2 et les Lignes directrices sur la divulgation des marchés.

Directive sur le réaménagement des effectifs

Est-ce que le soumissionnaire est un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu de la Directive sur le réaménagement des effectifs? **Oui** ( ) **Non** ( )

Si oui, le soumissionnaire doit fournir l'information suivante :

a) le nom de l'ancien fonctionnaire;

b) les conditions de l'incitatif versé sous forme de paiement forfaitaire;
c) la date de la cessation d'emploi;

d) le montant du paiement forfaitaire;
e) le taux de rémunération qui a servi au calcul du paiement forfaitaire;
f) la période correspondant au paiement forfaitaire, incluant la date du début, d'achèvement et le nombre de semaines;
g) le nombre et le montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réaménagement des effectifs.

Pour tous les contrats attribués pendant la période du paiement forfaitaire, le montant total des honoraires qui peut être payé à un ancien fonctionnaire qui a reçu un paiement forfaitaire est limité à 5 000 $, incluant les taxes applicables.

2.4 Demandes de renseignements – en période de soumission

a) Toutes les demandes de renseignements doivent être présentées à l'autorité contractante au plus tard cinq (5) jours civils avant la date de clôture des soumissions. Les demandes de renseignements reçues après cette date pourraient rester sans réponse.

b) Les soumissionnaires devraient indiquer aussi fidèlement que possible l'article numéroté de la demande de soumissions auquel se rapporte leur demande de renseignements. Ils doivent prendre soin d'expliquer chaque question en donnant suffisamment de détails pour permettre au Canada de fournir une réponse exacte. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque

élément pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et de permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les soumissionnaires.

2.5 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur selon les lois en vigueur en Ontario et les lois du Canada, le cas échéant.

Remarque à l'intention des soumissionnaires *:* À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées. *Les soumissionnaires doivent préciser sur le formulaire de présentation de la soumission, la province ou le territoire canadien de leur choix pour tout contrat subséquent.*

2.6 Améliorations apportées au besoin pendant la demande de soumissions

Si les soumissionnaires estiment pouvoir améliorer, techniquement ou technologiquement, le devis descriptif ou l'énoncé des travaux et l'énoncé des besoins contenus dans la demande de soumissions, sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer clairement les améliorations suggérées et les motifs qui les justifient. Les suggestions, qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier, seront examinées à la condition qu'elles soient soumises à l'autorité contractante conformément au paragraphe intitulé « Demandes de renseignements - en période de soumission ». Le Canada aura le droit d'accepter ou de rejeter n'importe quelle ou la totalité des suggestions proposées.

2.7 Données volumétriques

Les données ont été fournies aux soumissionnaires afin de les aider à préparer leurs soumissions. L'inclusion de ces données dans la présente demande de soumissions ne signifie pas que le Canada s'engage à ce que l'utilisation future de la solution logicielle de traitement des demandes d'AIPRP cadre avec ces données. Elles sont fournies strictement à titre informatif.

2.8 Processus de contestation des offres et mécanismes de recours

a) Les fournisseurs potentiels ont accès à plusieurs mécanismes pour contester des aspects du processus d'approvisionnement jusqu'à l'attribution du marché, inclusivement.

b) Le Canada invite les fournisseurs à porter d'abord leurs préoccupations à l'attention de l'autorité contractante. Le site Web du Canada Achats et ventes, sous le titre « Processus de contestation des soumissions et mécanismes de recours », fournit de l'information sur les organismes de traitement des plaintes possibles, notamment :
   - Bureau de l'ombudsman de l'approvisionnement (BOA)
   - Tribunal canadien du commerce extérieur (TCCE)

c) Les fournisseurs devraient savoir que des **délais stricts** sont fixés pour le dépôt des plaintes et qu'ils varient en fonction de l'organisation concernée. Les fournisseurs devraient donc agir rapidement s'ils souhaitent contester un aspect du processus d'approvisionnement.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

Les soumissions doivent être préparées conformément aux Instructions uniformisées des CCUA 2003 – Biens ou services – Exigences concurrentielles et aux articles décrits dans la partie 3 – Instructions pour la préparation des soumissions.

3.1 Instructions pour la préparation des soumissions

a) Si Le Canada demande que le soumissionnaire envoie sa soumission par voie électronique en conformité avec l'article 08 du Guide des clauses et conditions uniformisées d'achat (CCUA) 2003, Instructions uniformisées – biens ou services – besoins concurrentiels. Les répondants doivent présenter leur soumission en un seul message Connexion postel. Le service Connexion postel de la Société canadienne des postes peut recevoir plusieurs fichiers joints par message. La taille totale maximale d'un message individuel est de 1 Go, y compris les pièces jointes. Il est à noter qu'il faut avoir une adresse postale canadienne pour utiliser le service Connexion postel. Si le soumissionnaire n'en a pas, il peut utiliser l'adresse électronique de l'Unité de réception des soumissions, tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca, pour s'inscrire au service Connexion postel. Les soumissions envoyées directement à cette adresse courriel de l'Unité de réception des soumissions ne seront pas acceptées. Cette adresse courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel que décrit dans le document 2003, Instructions uniformisées, ou pour envoyer des soumissions dans un message Connexion postel si le soumissionnaire utilise son propre marché de licence pour Connexion postel.

b) Le soumissionnaire doit présenter les sections suivantes de sa soumission en un (1) document PDF :

Section I : Soumission technique (Tout le contenu, sauf autres types de fichiers)

Section II : Soumission financière

Section III : Attestations

Section IV: Renseignements Supplémentaires

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

c) Dans le cas où la DP précise que des fichiers autres que PDF sont requis dans la soumission, le soumissionnaire doit soumettre ces fichiers connexes en pièce jointe à l'unique message Connexion postel tel qu'indiqué ci-dessus. La taille totale maximale de ce message individuel est de 1 Go, y compris les pièces jointes.

d) Format de soumission **:** Le Canada demande aux soumissionnaires de suivre les instructions de présentation décrites ci-dessous pour la préparation de leur soumission :

(i) utiliser un système de numérotation qui correspond à la demande de soumissions; et

(ii) inclure une page de titre au recto de chaque volume de la soumission qui comprend le titre, la date, le numéro de la demande de soumissions, le nom et l'adresse du soumissionnaire et les coordonnées de son représentant.

3.2 Présentation d'une seule soumission

a) Un soumissionnaire, y compris ses entités liées, pourra participer dans la présentation :

(i) d'une soumission préparée par le soumissionnaire et d'une soumission préparée par une entité liée au soumissionnaire dans le cadre d'une coentreprise qui comprend au moins une entité qui n'est pas liée au soumissionnaire;

(ii) de deux soumissions préparées par des coentreprises; chacune de ces coentreprises devra comprendre une ou plusieurs entités liées au soumissionnaire. L'une des deux coentreprises devra compter au moins une entité non liée au soumissionnaire;

(iii) de deux soumissions, chacune étant présentée par le soumissionnaire et une entité liée.

b) Aux fins du présent article, peu importe la province ou le territoire où les entités visées ont été constituées en société ou formées juridiquement (qu'il s'agisse d'une personne physique, d'une société, d'un partenariat, etc.), une entité est considérée comme étant « liée » à un soumissionnaire, si :

(1) il s'agit de la même entité juridique (c'est-à-dire la même personne physique, personne morale ou société à responsabilité limitée, le même partenariat, etc.);

(2) il s'agit de « personnes liées » ou de « personnes affiliées » aux termes de la Loi de l'impôt sur le revenu du Canada;

(3) les entités entretiennent une relation fiduciaire (découlant d'une convention de mandat ou de toute autre forme de relation fiduciaire) ou en ont entretenu une au cours des deux années ayant précédé la clôture des soumissions;

(4) les entités n'ont pas autrement de lien de dépendance entre elles ou avec la même tierce partie.

c) Les membres individuels d'une coentreprise ne peuvent pas participer à une autre soumission en présentant eux-mêmes une soumission ou en participant à une autre coentreprise.

3.3 Expérience de la coentreprise

a) Lorsque le soumissionnaire est une coentreprise qui possède de l'expérience à ce titre, il peut soumettre l'expérience qu'il a acquise dans le cadre de cette coentreprise.

Exemple : Un soumissionnaire est une coentreprise formée des membres L et O. La demande de soumissions exige que le soumissionnaire possède de l'expérience en prestation de services de maintenance et dépannage à un client comptant au moins 10 000 utilisateurs pendant 24 mois. Le soumissionnaire (en tant que coentreprise formée des membres L et O) a déjà fourni ces services par le passé. Il peut donc citer cette expérience pour démontrer qu'il satisfait à cette exigence. Si L a acquis cette expérience alors qu'il était en coentreprise avec une tierce partie N, cette expérience ne peut pas être utilisée parce que N ne fait pas partie de la coentreprise qui présente une soumission.

b) Une coentreprise qui présente une soumission peut évoquer l'expérience de l'un de ses membres pour démontrer qu'elle satisfait à tout critère technique de la présente demande de soumissions.

Exemple : Un soumissionnaire est membre d'une coentreprise composée de X, Y et Z. Si, dans la demande de soumissions, on exige que : a) le soumissionnaire ait trois ans d'expérience dans la prestation de services de maintenance, et b) que le soumissionnaire ait deux ans d'expérience dans l'intégration de matériel dans des réseaux complexes, chacune de ces deux exigences peut être satisfaite par un membre différent de la coentreprise.

Cependant, pour un critère donné, par exemple celui qui concerne l'expérience de trois ans dans la prestation de services de maintenance, le soumissionnaire ne peut pas indiquer que chaque membre, soit X, Y et Z, a un an d'expérience pour un total de trois ans. Cette proposition serait jugée irrecevable.

c) Les membres de la coentreprise ne peuvent cependant pas mettre en commun leurs capacités pour répondre à un critère technique donné de la présente demande de soumissions. Un membre de la coentreprise peut néanmoins mettre sa propre expérience en commun avec celle de la coentreprise. Chaque fois qu'il doit faire la preuve qu'il répond à un critère, le soumissionnaire doit indiquer quel membre de la coentreprise y répond. Si le soumissionnaire ne l'a pas fait, l'autorité contractante permettra au soumissionnaire de fournir cette information pendant la période d'évaluation. Si le soumissionnaire ne fournit pas ce renseignement pendant la période fixée par l'autorité contractante, sa soumission sera déclarée non recevable.

Exemple : Un soumissionnaire est membre d'une coentreprise composée de A et B. Si, dans une demande de soumissions, on exige que le soumissionnaire ait de l'expérience dans la prestation de ressources pour un minimum de 100 jours facturables, le soumissionnaire peut démontrer son expérience en présentant ce qui suit :

- les contrats signés par A;
- les contrats signés par B; ou
- les contrats signés par A et B en coentreprise, ou
- les contrats signés par A et les contrats signés par A et B en coentreprise, ou
- les contrats signés par B et les contrats signés par A et B en coentreprise.

Le tout doit totaliser 100 jours facturables.

d) Les soumissionnaires qui ont des questions concernant l'évaluation des soumissions présentées par des coentreprises devraient les poser dans le cadre du processus de demande de renseignements, le plus tôt possible durant la période de soumission.

3.4 Section I : Soumission technique

a) Dans leur offre technique, les soumissionnaires doivent indiquer clairement le ou les niveaux de fonctionnalité qu'ils soumissionnent, et doivent démontrer qu'ils comprennent les exigences énoncées dans la demande de soumissions et expliquer la façon dont ils répondront à ces exigences. Ils doivent démontrer leur capacité d'effectuer les travaux de façon complète, concise et claire.

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

b) La soumission technique comprend ce qui suit :

1. **Formulaire de présentation des soumissions** : Les soumissionnaires doivent joindre à leur soumission le formulaire de présentation des soumissions (formulaire 1). Ce formulaire constitue un document général sur lequel les soumissionnaires peuvent fournir les renseignements exigés dans le cadre de l'évaluation de la soumission et de l'attribution du contrat, tels que le nom d'une personne-ressource et leur numéro d'entreprise – approvisionnement, etc. L'utilisation de ce formulaire pour présenter ces renseignements est recommandée, mais non obligatoire. Si le Canada considère que les renseignements demandés dans le formulaire de présentation de la soumission sont

incomplets ou doivent être corrigés, il donnera au soumissionnaire la possibilité de les compléter ou de les corriger.

2. **Documentation technique :** Le soumissionnaire est prié de fournir des documents techniques tels que des manuels d'utilisation, des captures d'écran, des démonstrations vidéo, des documents de conception ou de gestion du système (ou d'autres sources d'information) pour étayer sa réponse à chaque exigence. L'indication de liens vers des sites Web n'est pas acceptable, et dans le cas où une telle indication sert à confirmer une exigence obligatoire, la soumission peut considérer comme non conforme. Tout document de référence mentionné par le soumissionnaire pour démontrer la conformité à un critère doit faire partie de la soumission. Un document qui n'est pas joint à la soumission ne sera pas pris en considération par le Canada. Lorsque la référence n'est pas située, le Canada peut demander que le soumissionnaire dirige le Canada vers l'endroit approprié dans le document.

3. **Pour les projets antérieurs similaires :** Dans les cas où la soumission doit comprendre la description de projets antérieurs semblables : (i) le projet doit avoir été réalisé par le soumissionnaire lui-même (l'expérience acquise par un sous-traitant proposé ou une société affiliée au soumissionnaire ne compte pas); (ii) toutes les descriptions de projet doivent comprendre, au minimum, le nom et le numéro de téléphone ou l'adresse de courriel d'un client cité en référence; et (IIIe) dans l'éventualité où le soumissionnaire présente plus de projets semblables que ce qui a été demandé, le Canada aura le plein pouvoir de choisir ceux qui seront évalués. Un projet sera jugé « similaire » aux travaux à effectuer dans le cadre du contrat subséquent s'il porte sur des travaux qui correspondent étroitement aux descriptions indiquées à l'annexe A, Énoncé des travaux. Les travaux seront considérés comme « correspondant étroitement » si la description du projet inclut au moins 50 % des points de responsabilité figurant dans la description de la catégorie de ressources donnée.

4. **Coordonnées des clients cités en référence :**

   Le soumissionnaire doit fournir les coordonnées des clients. Chaque client cité en référence doit confirmer, à la demande de SPAC, les faits indiqués dans la soumission du soumissionnaire.

   Voici la forme de la question qui sera utilisée pour demander la confirmation des clients cités en référence :

   [Exemple de question destinée aux clients cités en référence : « [Nom du soumissionnaire] a-t-il offert des services de [décrire les services et, le cas échéant, les délais dans lesquels ces services doivent avoir été offerts] à votre organisation? »

   ____ Oui, le soumissionnaire a fourni à mon organisation les services décrits ci-dessus.

   ____ Non, le soumissionnaire n'a pas fourni à mon organisation les services décrits ci-dessus.

   ____ Je ne souhaite pas donner de renseignements sur les services décrits ci-dessus ou je ne suis pas en mesure de le faire.

   Pour chaque client cité en référence, le soumissionnaire doit, au minimum, fournir le nom et l'adresse de courriel d'une personne-ressource. Si seul le numéro de téléphone est fourni, il sera utilisé pour demander l'adresse de courriel, et la vérification des références se fera par courriel.

   Les soumissionnaires doivent en outre indiquer le titre de la personne-ressource du client. Il incombe au soumissionnaire de s'assurer que la personne-ressource qu'il propose est au fait des services qu'il a offerts et qu'elle est prête à être citée en référence. Les références de l'État sont acceptées.

5. **Liste de logiciels proposés qui feront partie de la solution :** Le soumissionnaire doit fournir une liste détaillée énumérant le nom et le numéro de version de chaque composante logicielle requise pour la solution proposée. Si la liste des logiciels sous licence proposés n'est pas incluse dans la soumission, elle doit être remise à l'autorité contractante avant l'attribution du contrat.

6. **Stratégie de mise à jour de logiciels :** Le soumissionnaire doit proposer une stratégie mise à jour de logiciels, laquelle devrait démontrer qu'elle répond à toutes les exigences de traitement décrites dans l'énoncé des travaux.

7. **Architecture du système de solution :** Le soumissionnaire doit inclure un aperçu de l'architecture technique de la solution logicielle proposée. Cela est demandé à titre d'information seulement et ne sera pas évalué.

8. **Description de l'évolution de la solution logicielle** : Le soumissionnaire doit décrire quand et comment la solution logicielle proposée a été conçue et comment elle a évolué, en précisant les caractéristiques de chaque version. Ces renseignements ne sont demandés qu'à titre indicatif et ne seront pas évalués.

9. **Solution de bac de sable** : Le soumissionnaire doit fournir une solution de bac de sable conformément à l'annexe J – Critères d'évaluation des soumissions.

3.5 Section II : Soumission financière

a) **Soumission financière :** Les soumissionnaires doivent présenter leur soumission financière conformément à la base de paiement à l'annexe B », sans aucune condition, hypothèse ou restriction. Toute soumission financière qui vise à restreindre la façon dont le Canada acquiert des biens ou des services en vertu du contrat subséquent, à l'exception des restrictions qui sont expressément énoncées dans la présente demande de soumissions, peut être considérée comme non recevable. Le montant total des taxes applicables doit être indiqué séparément, s'il y a lieu. À moins d'indication contraire, le soumissionnaire est prié d'inclure un prix ferme tout compris en dollars canadiens dans chaque cellule nécessitant une inscription dans les tableaux de prix.

b) **Fluctuation du taux de change :** La demande de soumissions ne prévoit aucune protection relative à la fluctuation du taux de change. Aucune demande de protection contre la fluctuation du taux de change ne sera prise en considération. Toutes les offres qui comprennent une telle disposition seront jugées non recevables.

c) **Variation des taux pour les ressources par période :** Pour toute catégorie de personnel donnée, si les tableaux financiers fournis par le Canada permettent de facturer différents prix fermes pour une catégorie de personnel, pendant des périodes différentes. Le taux proposé pour une même catégorie de ressources pour toute période subséquente ne doit pas être inférieur au taux présenté dans la soumission pour la période comprenant la première année d'option du contrat.

d) **Prix non indiqués :** On demande aux soumissionnaires d'indiquer « 0,00 $ CAN » pour tout élément qu'il ne compte pas facturer ou qui fait déjà partie d'autres prix présentés dans les tableaux. Si le soumissionnaire laisse le champ en blanc, le Canada considérera le prix comme étant « 0,00 $ CDN » aux fins d'évaluation et pourrait demander au soumissionnaire de confirmer que le prix est bel et bien 0,00 $ CDN. Aucun soumissionnaire ne sera autorisé à ajouter ni à modifier un prix durant cette confirmation. Si le soumissionnaire refuse de confirmer que le prix d'un champ vierge est de 0,00 $ CDN, sa soumission sera déclarée non recevable.

e) **Soumission financière :** La soumission financière doit inclure tous les coûts liés au besoin décrit dans la demande de soumissions pour toute la période du contrat, y compris toute option de prolongation de la période du contrat. Les soumissionnaires doivent présenter les prix, y compris les prix associés à l'équipement, aux logiciels, aux périphériques, au câblage et aux composantes nécessaires pour répondre aux exigences de la demande de soumissions, conformément à l'annexe B - Base de paiement..

f) **Paiement électronique de factures – Soumission :** Si vous êtes disposé à accepter les paiements de factures effectués à l'aide des instruments de paiement électronique, remplissez l'annexe I – Formulaires du soumissionnaire, formulaire 8 – Instruments de paiement électronique afin d'indiquer les instruments qui sont acceptés.

Si l'annexe I – Formulaires du soumissionnaire, formulaire 8 – Instruments de paiement électronique, n'est pas remplie, on partira du principe que les instruments de paiement électronique ne sont pas acceptés pour le paiement des factures.

3.6 Section III : Attestations

Les soumissionnaires doivent présenter les attestations et les renseignements supplémentaires indiqués dans la partie 5.

3.7 Section IV : Renseignements supplémentaires

3.7.1 Installations ou locaux proposés par le soumissionnaire nécessitant des mesures de sauvegarde

Comme il est indiqué à la partie 1, à la rubrique sur les exigences relatives à la sécurité, le soumissionnaire doit fournir les adresses complètes de ses sites ou de ses locaux, ou des sites ou des locaux des personnes proposées, pour lesquels des mesures de sauvegarde sont requises pour l'exécution des travaux.

Numéro civique, nom de la rue, numéro d'unité, de bureau ou d'appartement
Ville, province, territoire ou État
Code postal/code ZIP
Pays

L'agent de sécurité de l'entreprise doit s'assurer, dans le cadre du Programme de sécurité des contrats, que l'entrepreneur et les individus détiennent une autorisation de sécurité en règle, au niveau approprié, comme indiqué à la partie 1, disposition 1.1, Exigences relatives à la sécurité.

Bidders are requested to indicate this information on their Bid Submission Form.

3.7.2 Exigences relatives à la sécurité de la chaine d'approvisionnement

Les soumissionnaires doivent satisfaire aux exigences touchant l'information sur la sécurité de la chaîne d'approvisionnement (ISCA) décrites à l'annexe F – Processus d'intégrité de la chaîne d'approvisionnement. Le Canada utilisera l'ISCA pour évaluer si, à son avis, la chaîne d'approvisionnement proposée par un soumissionnaire pourrait faire en sorte que la solution proposée par le soumissionnaire compromette ou serve à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, selon le Processus d'intégrité de la chaîne d'approvisionnement (Annexe F).

3.7.3 Prise en compte des conditions supplémentaires d'utilisation du logiciel inclus dans la soumission

1. L'acceptation de l'ensemble des modalités figurant à la partie 7 – Clauses du contrat subséquent (y compris les clauses relatives à la licence d'utilisation du logiciel et les

clauses incorporées par renvoi) constitue une exigence obligatoire de la présente demande de soumissions.

2. Toutefois, les soumissionnaires peuvent, dans le cadre de leur soumission, présenter des modalités supplémentaires d'utilisation du logiciel. L'inclusion ou non de ces modalités d'utilisation du logiciel dans tout contrat subséquent (en tant qu'annexe, conformément à l'article intitulé « Ordre de priorité des documents » dans les clauses du contrat subséquent) sera déterminée à l'aide du processus décrit ci-après. Quant à savoir si les modalités supplémentaires d'utilisation du logiciel proposées sont acceptables pour le Canada, la décision est entièrement à la discrétion du Canada. Le processus est le suivant :
   (i) Les soumissions peuvent comprendre des modalités supplémentaires d'utilisation du logiciel, qui sont proposées pour compléter les modalités des clauses du contrat subséquent. Les soumissionnaires ne devraient pas présenter les modalités standard de licence intégrales de l'éditeur de logiciels (parce que les modalités standard de licence intégrales contiennent généralement des dispositions qui ne traitent pas uniquement de l'utilisation du logiciel; par exemple, elles traitent souvent de questions telles que la limite de la responsabilité ou la limite de garantie qui ne constituent pas des modalités d'utilisation du logiciel);
   (ii) Dans les cas où un soumissionnaire a présenté les modalités standard de licence intégrales de l'éditeur de logiciels, le Canada exigera que le soumissionnaire retire ces modalités et qu'il présente seulement les modalités d'utilisation du logiciel qu'il souhaite que le Canada prenne en considération;
   (iii) Le Canada examinera toutes les modalités supplémentaires d'utilisation du logiciel proposées par les 3 soumissionnaires les mieux classés (après l'évaluation financière) afin de déterminer si certaines des dispositions proposées par quelconque soumissionnaire sont inacceptables pour le Canada;
   (iv) Si le Canada détermine qu'une modalité d'utilisation du logiciel proposée par un soumissionnaire est inacceptable, il avisera le soumissionnaire, par écrit, et lui fournira l'occasion de retirer cette disposition de sa soumission ou de proposer une formulation de remplacement à des fins d'examen. Le Canada peut préciser un délai de réponse au soumissionnaire. Si le soumissionnaire présente une nouvelle formulation que le Canada juge inacceptable, le Canada n'est pas obligé de lui fournir une autre occasion de proposer une formulation de remplacement;
   (v) If Si le soumissionnaire refuse de retirer les dispositions inacceptables pour le Canada de sa soumission dans le délai prescrit par le Canada dans son avis, la soumission sera jugée irrecevable et rejetée; le Canada peut alors passer à la soumission classée au rang suivant; et
   (vi) Si le soumissionnaire accepte de retirer les dispositions inacceptables pour le Canada et qu'il se voit attribuer tout contrat subséquent, les modalités supplémentaires d'utilisation du logiciel (dans leur version modifiée) seront intégrées au contrat en tant qu'annexe, conformément à l'article intitulé « Ordre de priorité des documents » dans les clauses du contrat subséquent.

3. Pour plus de certitude et afin de garantir que seules les modalités supplémentaires d'utilisation du logiciel qui ont été approuvées par les deux parties soient incorporées dans tout contrat subséquent, à moins que les modalités supplémentaires d'utilisation du logiciel proposées par le soumissionnaire ne soient jointes en tant qu'annexe distincte au contrat et paraphées par les deux parties, elles ne seront pas considérées comme faisant partie de tout contrat subséquent (même si elles font partie de la soumission qui est incorporée par renvoi dans le contrat). Le fait que certaines conditions ou modalités d'utilisation du logiciel supplémentaires soient incluses dans la soumission n'entraîne pas l'application de ses modalités au contrat subséquent, que le Canada s'oppose ou non à ces modalités conformément à la procédure ci-dessus.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

a) L'évaluation sera menée d'une manière structurée, uniforme, impartiale, équitable et transparente. L'objectif de l'évaluation est de déterminer, sur la base d'un dossier bien étayé, la soumission qui offre la meilleure valeur au Canada.

b) Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les exigences techniques et financières. À la fin de l'évaluation des soumissions, jusqu'à trois soumissionnaires ayant obtenu les meilleurs résultats seront pris en considération pour l'attribution d'un contrat pour les travaux de la phase 1 visant à élaborer une solution prototype pour une évaluation de la capacité et de la convivialité (ÉCC).

c) Le processus d'évaluation et de sélection se déroulera en plusieurs étapes. Même si l'évaluation et la sélection seront effectuées par étapes, le fait que le Canada soit passé à une étape ultérieure de ses évaluations ne signifie pas que le Canada a irréfutablement déterminé que le soumissionnaire ou l'entrepreneur a réussi toutes les étapes précédentes. Le Canada peut mener certaines étapes de l'évaluation simultanément.

d) Les équipes d'évaluation seront composées de représentants du client et de SPAC qui évalueront les soumissions et les prototypes au nom du Canada. Le Canada peut faire appel à des experts-conseils indépendants ou à des personnes-ressources du gouvernement pour évaluer les soumissions et tout prototype. Tous les membres des équipes d'évaluation ne participeront pas nécessairement à tous les aspects de l'évaluation de l'étape concernée.

e) En plus de tout autre délai prescrit dans la demande de soumissions :

(1) **Demandes de précisions :** Si le gouvernement du Canada demande des précisions au soumissionnaire sur sa proposition ou s'il veut vérifier celle-ci, le soumissionnaire disposera d'un délai de 2 jours ouvrables (ou d'un délai plus long spécifié par écrit par le titulaire du pouvoir de passation des marchés) pour fournir les renseignements demandés. À défaut de respecter ce délai, la soumission sera jugée non recevable.

(2) **Demandes de renseignements supplémentaires** : Si le Canada demande d'autres renseignements pour l'une des raisons qui suivent (selon la section intitulée « Déroulement de l'évaluation » du document 2003, Instructions uniformisées – biens ou services – besoins concurrentiels) :

i. vérifier tout renseignement fourni par le soumissionnaire dans sa soumission;
ii. communiquer avec une ou l'ensemble des références citées par le soumissionnaire (références citées dans les curriculum vitæ des ressources individuelles) afin de valider les renseignements fournis par le soumissionnaire.

Le soumissionnaire doit soumettre les renseignements demandés par le Canada dans les deux (2) jours ouvrables suivant la demande de l'autorité contractante. Si le soumissionnaire ne respecte pas ce délai ou ne fournit pas d'autres renseignements, la soumission pourrait être déclarée non recevable.

(3) Prolongation des délais : Si le soumissionnaire a besoin d'un délai supplémentaire, l'autorité contractante pourra le lui accorder, à sa seule et entière discrétion.

f) Le Canada utilisera le processus de conformité des soumissions par étapes (PCSE) décrit ci-dessous.

4.1.1. Processus de conformité des soumissions par étapes (PCSE)

4.1.1.1 Généralités

a) Le Canada suit le PCSE décrit ci-dessous pour ce besoin. Nonobstant tout examen effectué par le Canada à l'étape I ou II du PCSE, les soumissionnaires sont et resteront les seuls responsables de l'exactitude, de la cohérence et de l'intégralité de leurs soumissions, et le Canada n'assume, à la suite de cet examen, aucune obligation ou responsabilité de repérer toute erreur ou omission dans les soumissions ou dans les réponses d'un soumissionnaire à toute communication du Canada.

LE SOUMISSIONNAIRE RECONNAÎT QUE LES EXAMENS AUX ÉTAPES I ET II DU PCSE SONT PRÉLIMINAIRES ET N'EMPÊCHENT PAS QU'UNE SOUMISSION SOIT JUGÉE NON RECEVABLE À L'ÉTAPE III, ET CE, MÊME POUR LES EXIGENCES OBLIGATOIRES QUI ONT FAIT L'OBJET D'UN EXAMEN AU COURS DE LA'ÉTAPE I OU II, ET MÊME SI LA SOUMISSION AVAIT ÉTÉ JUGÉE RECEVABLE À L'UNE DE CES ÉTAPES PRÉCÉDENTES. LE CANADA PEUT JUGER QU'UNE SOUMISSION NE RÉPOND PAS À UNE EXIGENCE OBLIGATOIRE À N'IMPORTE QUELLE ÉTAPE.

LE SOUMISSIONNAIRE RECONNAÎT ÉGALEMENT QUE SA RÉPONSE À UN AVIS OU À UN RAPPORT SUR L'ÉVALUATION DE LA CONFORMITÉ (REC) [CES TERMES SONT DÉFINIS PLUS BAS] À L'ÉTAPE I OU II, POURRAIT NE PAS RÉPONDRE AUX EXIGENCES OBLIGATOIRES QUI FONT L'OBJET DE L'AVIS OU DU REC ET POURRAIT RENDRE SA SOUMISSION NON CONFORME À D'AUTRES EXIGENCES OBLIGATOIRES.

b) Le Canada peut, à sa discrétion et à tout moment, demander et accepter de l'information du soumissionnaire pour corriger des erreurs ou des lacunes administratives dans la soumission, et peut considérer que cette information fait partie de la soumission. Ces erreurs pourraient être, entre autres : une signature manquante; une case non cochée dans un formulaire; une erreur de format ou de forme; l'omission de l'accusé de réception, du numéro d'entreprise – approvisionnement ou les coordonnées des personnes-ressources, comme les noms, les adresses et les numéros de téléphone; des erreurs commises par inadvertance dans les chiffres ou les calculs qui ne modifient pas le montant que le soumissionnaire a indiqué pour le prix ou tout composant visé par l'évaluation. Cela ne limitera pas son droit d'exiger ou d'accepter tout autre renseignement après la clôture de la demande de soumissions dans des cas où la demande de soumissions le permet expressément. Le soumissionnaire disposera de la période précisée par écrit par le Canada pour fournir la documentation nécessaire. À défaut de respecter ce délai, sa soumission sera jugée non recevable.

c) Le processus de conformité des soumissions par étapes ne limite pas les droits du Canada en vertu du Guide des Clauses et conditions uniformisées d'achat 2003 (2019-03-04) Instructions uniformisées – biens ou services – besoins concurrentiels, ni le droit du Canada de demander ou d'accepter toute information pendant la période de soumission ou après la clôture de cette dernière, lorsque la demande de soumissions confère expressément ce droit au Canada, ou dans les circonstances prévues à l'alinéa (b).

d) Le Canada enverra un avis ou un REC par la méthode de son choix et à sa discrétion absolue. Le soumissionnaire doit soumettre sa réponse par la méthode décrite dans l'avis ou le REC. Les réponses sont réputées avoir été reçues par le Canada à la date et à l'heure auxquelles elles ont été livrées au Canada par la méthode indiquée dans l'avis ou le REC et à l'adresse qui y figure. Un courriel de réponse autorisé dans l'avis ou le REC est réputé reçu par le Canada à la date et à l'heure auxquelles il a été reçu dans la boîte de réception de l'adresse électronique indiquée dans l'avis ou le REC. Un avis, ou un REC, envoyé par le Canada au soumissionnaire à l'adresse fournie par celui-ci dans la soumission ou après l'envoi de celle-ci est réputé avoir été reçu par le soumissionnaire à la date à laquelle il a été envoyé par le Canada. Le Canada n'est pas responsable de la réception tardive d'une réponse par le Canada, quelle qu'en soit la cause.

4.1.1.2 Étape I du PCSE : Soumission financière

a) Après la date et l'heure de clôture de la présente demande de soumissions, le Canada examinera la soumission afin de déterminer si elle comprend une soumission financière et si la soumission financière comprend tous les renseignements requis dans la présente demande de soumissions. L'examen de la soumission par le Canada à l'étape I se limitera à déterminer si les renseignements requis dans la soumission financière de la demande de soumissions sont manquants. Cet examen ne déterminera pas si la soumission financière respecte toute norme ou répond à toutes les exigences de la demande de soumissions.

b) L'examen par le Canada à l'étape I sera réalisé par des représentants du ministère de Services publics et Approvisionnement Canada.

c) Si le Canada détermine, à sa discrétion absolue, qu'il n'y a pas de soumission financière ou que la soumission financière ne contient aucun des renseignements requis selon la demande de soumissions, la soumission sera jugée non recevable et rejetée d'emblée.

d) Pour les soumissions autres que celles décrites au point c), le Canada fera parvenir un avis écrit au soumissionnaire (« Avis ») indiquant quels renseignements sont manquants dans la soumission financière. Un soumissionnaire dont la soumission financière a été déclarée conforme aux exigences qui font l'objet d'un examen à l'étape I ne recevra pas d'avis. De tels soumissionnaires ne sont pas autorisés à soumettre des renseignements supplémentaires relativement à leur soumission financière.

e) Les soumissionnaires auxquels un avis a été envoyé disposeront de la période de temps précisée dans l'avis (la « période de correction ») en vue de corriger les problèmes signalés dans l'avis en fournissant au Canada, par écrit, des renseignements supplémentaires ou des précisions en réponse à l'avis. Les réponses reçues après la fin de la période de correction ne seront pas prises en compte par le Canada, sauf dans les circonstances et selon les modalités expressément prévues dans l'avis.

f) Dans sa réponse à l'avis, le soumissionnaire ne sera autorisé à corriger que la partie de sa soumission financière qui est indiquée dans l'avis. Par exemple, lorsque l'avis indique qu'un élément devant être rempli est laissé en blanc, seuls les renseignements manquants peuvent être ajoutés à la soumission financière, sauf lorsque l'ajout de tels renseignements entraîne nécessairement une modification à d'autres calculs précédemment soumis dans sa soumission financière (p. ex. le calcul visant à déterminer un prix total). De tels ajustements doivent être indiqués par le soumissionnaire, et seuls ces ajustements peuvent être effectués. Tous les renseignements fournis doivent satisfaire aux exigences de la demande de soumissions.

g) Toute autre modification apportée à la soumission financière par le soumissionnaire sera considérée comme un nouveau renseignement et sera écartée. Aucun changement ne sera autorisé à une autre section de la soumission du soumissionnaire. L'information soumise conformément aux exigences de cette demande de soumissions en réponse à l'avis remplacera, en intégralité, **uniquement** la partie de la soumission financière originale telle qu'il est autorisé ci-dessus, et sera utilisée pour le reste du processus d'évaluation des soumissions.

h) Le Canada déterminera si la soumission financière est conforme aux exigences évaluées à l'étape I, en tenant compte des renseignements supplémentaires ou des précisions qui peuvent avoir été fournis par le soumissionnaire conformément au présent article. Si la soumission financière n'est pas conforme aux exigences évaluées à la étape I à la satisfaction du Canada, la soumission sera jugée irrecevable et sera rejetée d'emblée.

i) Seules les soumissions jugées conformes aux exigences de l'étape I à la satisfaction du Canada recevront une évaluation à l'étape II.

4.1.1.3 Étape II du PCSE : Soumission technique

a) L'examen du Canada au cours de l'étape II se limitera à une évaluation de la soumission technique afin de vérifier si le soumissionnaire n'a pas respecté l'une ou l'autre des exigences obligatoires d'admissibilité. Cet examen ne déterminera pas si la soumission technique respecte toute norme ou répond à toutes les exigences de la demande de soumissions. Les exigences obligatoires d'admissibilité sont les critères techniques obligatoires décrits dans la présente demande de soumissions comme faisant partie du PCSE. Les critères techniques obligatoires qui ne sont pas établis dans la présente demande d'offres comme étant assujettis au PCSE ne seront évalués qu'à l'étape III.

b) Le Canada enverra un avis écrit au soumissionnaire (Rapport d'évaluation de la conformité ou « REC ») indiquant les critères obligatoires admissibles auxquels la soumission n'a pas satisfait. Un soumissionnaire dont la soumission a été jugée conforme aux exigences examinées à l'étape II recevra un REC, attestant que sa soumission a été jugée conforme aux exigences évaluées à l'étape II. Un tel soumissionnaire n'est pas autorisé à présenter une réponse au REC.

c) Le soumissionnaire disposera de la période précisée dans le REC (« période de correction ») pour remédier au défaut de satisfaire à tout critère obligatoire admissible indiqué dans le REC en fournissant au Canada, par écrit, des renseignements supplémentaires ou différents ou des précisions en réponse au REC. Les réponses reçues après la fin de la période de correction ne seront pas prises en compte par le Canada, sauf dans les circonstances et selon les modalités expressément prévues dans le REC.

d) La réponse du soumissionnaire doit aborder uniquement les critères obligatoires admissibles précisés dans le REC qui n'ont pas été respectés, et doit comprendre uniquement les renseignements qui sont nécessaires pour les respecter. Les renseignements supplémentaires fournis par le soumissionnaire qui ne sont pas nécessaires à la satisfaction de ces exigences ne seront pas pris en compte par le Canada, sauf lorsque la réponse aux critères obligatoires admissibles précisés dans le REC entraîne nécessairement une modification consécutive dans d'autres composantes de la demande de soumissions, le soumissionnaire doit définir ces modifications supplémentaires, à condition que sa réponse ne comprenne aucune modification à la soumission financière.

e) La réponse du soumissionnaire au REC devrait préciser, dans tous les cas, le critère obligatoire admissible du REC auquel il répond, y compris l'indication de la section correspondante de la soumission originale, le libellé de la modification proposée à cette section, ainsi que le libellé et l'emplacement dans la soumission de toute autre modification consécutive qui découle nécessairement de cette modification. Pour chaque modification corrélative, le soumissionnaire doit inclure une justification expliquant en quoi cette modification corrélative est une conséquence nécessaire de la modification proposée pour répondre au critère obligatoire admissible. Ce n'est pas au Canada qu'il incombe de réviser la soumission du soumissionnaire, et le défaut du soumissionnaire de le faire, conformément au présent sous-paragraphe, est à ses propres risques. Tous les renseignements fournis doivent satisfaire aux exigences de la demande de soumissions.

f) Toute modification à la soumission présentée par le soumissionnaire d'une façon qui n'est pas permise par la présente demande de soumissions sera considérée comme une nouvelle information et ne sera pas prise en considération. Les renseignements fournis conformément aux exigences de la présente demande de soumissions en réponse au REC remplaceront, en totalité, **uniquement** la partie de la soumission originale comme le permet cette section.

g) Les renseignements supplémentaires ou différents soumis au cours de l'étape II et permis par la présente section seront considérés comme étant inclus dans la soumission, mais ne seront pris en compte par le Canada dans l'évaluation de la soumission à l'étape II que pour déterminer si la soumission respecte les critères obligatoires admissibles. Ces renseignements ne seront utilisés à aucune autre phase de l'évaluation pour augmenter les notes que la soumission originale pourrait obtenir sans cet avantage. Par exemple, un critère obligatoire admissible qui exige l'obtention d'un nombre minimum de points pour être

considéré comme conforme sera évalué à l'étape II afin de déterminer si cette note minimum obligatoire aurait été obtenue si le soumissionnaire n'avait pas soumis les renseignements supplémentaires ou différents en réponse au REC. Dans ce cas, la soumission sera considérée comme étant conforme par rapport à ce critère obligatoire admissible, et les renseignements supplémentaires ou différents soumis par le soumissionnaire lieront le soumissionnaire dans le cadre de sa soumission, mais la note originale du soumissionnaire, qui était inférieure à la note minimum obligatoire pour ce critère obligatoire admissible, ne changera pas, et c'est cette note originale qui sera utilisée pour calculer les notes pour la soumission.

h) Le Canada déterminera si la soumission est conforme aux exigences évaluées à l'étape II, en tenant compte des renseignements supplémentaires ou différents ou des précisions qui peuvent avoir été fournis par le soumissionnaire conformément à la présente section. Si la soumission n'est pas conforme aux exigences évaluées à l'étape II à la satisfaction du Canada, la soumission sera jugée irrecevable et sera rejetée d'emblée.

i) Seules les soumissions jugées conformes aux exigences évaluées à l'étape II à la satisfaction du Canada feront l'objet d'une évaluation à l'étape III.

4.1.1.4 (2018-03-13) Étape III du PCSE : Évaluation finale de la soumission

a) Au cours de l'étape III, le Canada évaluera toutes les soumissions jugées conformes aux exigences évaluées à l'étape II. Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, y compris les critères d'évaluation techniques et financiers.
b) Une soumission est irrecevable et sera rejetée d'emblée si elle ne satisfait pas à tous les critères d'évaluation obligatoires de la demande de soumissions.

4.1.2 Évaluation

4.1.2.1 Critères techniques obligatoires :

a) Le processus de conformité des soumissions par étapes (PCSE) s'appliquera à tous les critères techniques obligatoires énumérés dans l'annexe J, Évaluation technique.
b) Les critères obligatoires qui seront évalués dans le cadre de l'évaluation de la soumission sont énumérés dans l'annexe J, Évaluation technique. Les soumissionnaires sont tenus d'indiquer clairement et avec suffisamment de détails tous les critères d'évaluation obligatoires en fonction desquels leur soumission sera évaluée. Il ne suffit pas de simplement reprendre les énoncés contenus dans les critères obligatoires.
c) Chaque soumission fera l'objet d'un examen pour en déterminer la conformité aux exigences obligatoires de la demande de soumissions. Tous les éléments de la demande de soumissions désignés précisément par les termes « doit », « doivent » ou « obligatoire » constituent des exigences obligatoires. Sous réserve du PCSE, les soumissions qui ne respecteront pas chaque exigence obligatoire seront déclarées irrecevables et rejetées.
d) Si une soumission énonce qu'une version ultérieure d'un produit qu'elle cite satisfera aux exigences obligatoires de la demande de soumissions, et que cette version ultérieure n'est pas disponible à la date de clôture des soumissions, la soumission sera rejetée.

4.1.2.2 Critères techniques cotés :

a) Les critères cotés qui seront évalués au cours de l'évaluation des soumissions sont énumérés à l'annexe J, Évaluation technique. Sous réserve du Processus de conformité des soumissions par étapes (PCSE), un soumissionnaire doit obtenir au moins 70 % de la note totale pour les critères d'évaluation technique énoncés à l'annexe J, Évaluation technique. Lesquels sont assujettis à une cote numérique.

b) Chaque soumission sera cotée en attribuant une note aux exigences cotées, lesquelles sont précisées dans la demande de soumissions par le terme « cotées » ou au moyen d'un renvoi à une note. Les soumissionnaires qui ne présentent pas des soumissions complètes contenant tous les renseignements exigés dans la demande de soumissions verront leurs soumissions cotées en conséquence. Les critères techniques cotés sont décrits à l'annexe J, Évaluation technique.

4.1.2.3 Vérification des références :

a) Le Canada vérifiera les références par courriel. Le Canada acheminera toutes les demandes de vérification des références par courriel le même jour aux personnes-ressources citées en référence par tous les soumissionnaires en utilisant les adresses de courriel fournies dans la soumission. La réponse doit être envoyée dans les cinq jours ouvrables suivant l'envoi du courriel de vérification des références, faute de quoi le Canada n'attribuera aucun point ou considérera que le soumissionnaire ne satisfait pas à l'exigence obligatoire en matière d'expérience (selon le cas).

b) Le troisième jour ouvrable après l'envoi de la demande de vérification d'une référence, si le Canada n'a toujours pas reçu de réponse, il en informera le soumissionnaire par courriel pour que ce dernier puisse rappeler à la personne en question qu'elle doit répondre au Canada dans le délai de cinq (5) jours ouvrables prescrit. Si la personne nommée par un soumissionnaire comme personne-ressource n'est pas disponible lorsque requise pendant la période d'évaluation, le soumissionnaire peut fournir le nom et l'adresse courriel d'une autre personne-ressource pour le même client. Cette possibilité ne sera offerte aux soumissionnaires qu'une fois par client et uniquement si la personne nommée initialement n'est pas disponible (c'est-à-dire que le soumissionnaire ne pourra pas soumettre le nom d'une autre personne si la première personne-ressource indique qu'elle ne souhaite pas répondre ou qu'elle n'est pas en mesure de le faire). Le soumissionnaire disposera de 24 heures pour soumettre le nom d'une nouvelle personne-ressource. Celle-ci aura de nouveau cinq (5) jours ouvrables pour répondre au Canada à compter de la date d'envoi de la demande de vérification des références.

c) En cas de contradiction entre l'information fournie par le soumissionnaire et celle fournie par la personne-ressource (référence), l'information fournie par la personne-ressource sera évaluée.

d) On n'accordera aucun point ou on ne considérera pas qu'un critère d'expérience obligatoire a été respecté (le cas échéant) si 1) le client cité en référence indique qu'il n'est pas en mesure de fournir l'information demandée ou qu'il ne veut pas le faire ou que 2) le client cité en référence n'est pas un client du soumissionnaire même (par exemple, le client ne peut pas être le client d'une filiale du soumissionnaire). De même, on n'accordera aucun point au soumissionnaire ou on ne considérera pas qu'un critère obligatoire a été respecté si le client est lui-même une filiale ou autre entité qui a des liens de dépendance avec le soumissionnaire.

e) La vérification des références est discrétionnaire. Toutefois, si SPAC choisit d'effectuer une vérification des références pour une exigence cotée ou obligatoire donnée, il vérifiera les références pour cette exigence pour tous les soumissionnaires qui n'ont pas, à ce moment-là, été jugés non recevables.

4.1.2.4 Évaluation financière

a) Les soumissionnaires doivent présenter leur soumission financière en conformité avec la base de paiement reproduite à l'annexe B, servant uniquement à déterminer le prix évalué de chaque soumission. Les estimations qui servent à calculer le prix total de la soumission

sont des estimations seulement et ne doivent pas être considérées comme un engagement de la part du Canada.

b) **Formules figurant dans les tableaux des prix**. Si les tableaux d'établissement des prix fournis aux soumissionnaires à l'annexe B comprennent une formule, le Canada peut entrer les prix du formulaire fourni par les soumissionnaires dans un nouveau formulaire, si le Canada estime que la formule ne fonctionne plus correctement selon la version fournie par le soumissionnaire.

c) **Justification des tarifs des services professionnels.** Selon l'expérience du Canada, les soumissionnaires proposent de temps à autre des tarifs au moment de déposer une soumission pour une ou plusieurs catégories de personnel qu'ils refusent d'honorer par la suite, parce que ces tarifs ne leur permettent pas de recouvrer leurs propres coûts ou de réaliser un profit. Au moment d'évaluer les taux pour les services professionnels, le Canada peut, sans toutefois y être obligé, demander une justification des prix conformément au présent article. Si le Canada demande une justification de prix, elle sera demandée à tous les soumissionnaires conformes proposant un tarif au moins 20 % inférieur à la médiane des tarifs offerts par tous les soumissionnaires conformes pour la ou les mêmes catégories de ressources. Si le Canada demande une justification des prix, le soumissionnaire doit fournir les renseignements suivants :

(1.) une facture (ainsi que le numéro de série du contrat ou tout autre identifiant de contrat unique) démontrant que le soumissionnaire a fourni et facturé des services similaires à ceux qui seraient fournis par cette catégorie de ressources à un client (qui n'a aucun lien de dépendance avec le soumissionnaire), que les services ont été offerts pour une période d'au minimum trois mois au cours des douze mois précédant la date de clôture de la présente demande de soumissions, et que les tarifs facturés étaient égaux ou inférieurs à celui proposé au Canada;

(2.) relativement à la facture mentionnée en (i), une preuve du client du soumissionnaire démontrant que les services indiqués sur la facture comprennent au minimum de 50 % des tâches énumérées dans l'Énoncé des travaux pour la catégorie de ressources évaluée, et ce, à un taux déraisonnablement bas. Il peut s'agir d'une copie du contrat (dans lequel on décrit les services à offrir et où l'on démontre qu'au moins 50 % des tâches sont les mêmes que celles qui doivent être effectuées conformément à l'Énoncé des travaux de la présente demande de soumissions), ou d'une attestation du client indiquant que les services notés sur la facture comprenaient au moins 50 % des tâches qui doivent être effectuées conformément de l'Énoncé des travaux de la présente demande de soumissions);

(3.) pour chacun des contrats pour lesquels une facture est présentée à titre de justification, le curriculum vitæ de la ressource qui a offert les services dans le cadre de ce contrat afin de démontrer que la ressource répondrait aux exigences obligatoires et obtiendrait la note de passage pour tous les critères cotés;

(4.) le nom, le numéro de téléphone et, si possible, l'adresse de courriel d'une personne-ressource du client ayant reçu chacune des factures présentées au point (i), afin que le Canada puisse valider tout renseignement fourni par le soumissionnaire.

Lorsque le Canada demande une justification des tarifs offerts pour une catégorie de ressource particulière, il revient au soumissionnaire de présenter l'information (soit l'information décrite ci-haut ou d'autres renseignements, à la demande du Canada, y compris des renseignements qui lui permettraient de vérifier de l'information auprès de la ressource proposée) qui permettra au Canada de déterminer s'il peut compter en toute confiance sur la capacité du soumissionnaire à offrir les services requis aux tarifs

indiqués. Si le Canada considère que les renseignements fournis par le soumissionnaire ne permettent pas de justifier des taux déraisonnablement bas, la soumission sera jugée irrecevable.

1. Nombre de catégories de ressource évaluées: Toutes les catégories de ressources proposées seront évaluées dans le cadre de cette demande de soumissions. Les ressources supplémentaires ne seront évaluées qu'après l'attribution du contrat quand l'entrepreneur devra accomplir des tâches précises. Après l'attribution du contrat, le processus d'autorisation des tâches (AT) sera appliqué conformément à la Partie 7 – Clauses du contrat subséquent, selon l'article intitulé « Autorisation des tâches ». Lorsqu'un formulaire d'autorisation de tâche (formulaire d'AT) sera émis, l'entrepreneur devra proposer une ressource pour satisfaire au besoin précis d'après l'Énoncé des travaux du formulaire d'AT.

2. Corrections: Le Canada peut, à sa discrétion et à tout moment, demander et accepter de l'information du soumissionnaire pour corriger des erreurs ou des lacunes administratives dans la soumission, et peut considérer que cette information fait partie de la soumission. Ces erreurs pourraient être, entre autres : une signature manquante; une case non cochée dans un formulaire; une erreur de format ou de forme; l'omission de l'accusé de réception, du numéro d'entreprise – approvisionnement ou les coordonnées des personnes-ressources, comme les noms, les adresses et les numéros de téléphone; des erreurs commises par inadvertance dans les chiffres ou les calculs qui ne modifient pas le montant que le soumissionnaire a indiqué pour le prix ou tout composant visé par l'évaluation. Cela ne limite pas le droit du Canada d'exiger ou d'accepter tout renseignement après la date de présentation des soumissions lorsque la DP le permet expressément. Le soumissionnaire disposera de la période précisée par écrit par le Canada pour fournir la documentation nécessaire. À défaut de respecter ce délai, sa soumission sera jugée non conforme.

4.1.2.5 Classement des soumissions

1. **Note combinée la plus élevée - technique (70%) et prix (30%)**

Après l'évaluation par le Canada des soumissions techniques et financières, les trois soumissions les mieux classées seront déterminées sur la base de la note la plus élevée attribuée à la fois à la valeur technique et au prix. Une pondération de 70 % sera attribuée à la soumission technique et de 30 % à la soumission financière selon la formule suivante :

$$\frac{\text{Total des points reçus par le soumissionnaire pour exigences cotées}}{\text{Note technique maximale possible}} \times 70\% = \text{Total 1}$$

$$\frac{\text{Prix total le plus bas}}{\text{Prix total de la soumission classée}} \times 30\ \% = \text{Total 2}$$

Somme de (total 1) et de (total 2) = note combinée du mérite technique et du prix.

Composantes de l'évaluation	Pondération globale
Note de la soumission technique	70%

Note de la soumission financière	30%

La soumission conforme qui obtiendra la meilleure note sera celle qui satisfait à tous les critères obligatoires et qui présente la meilleure évaluation combinée de mérite technique et de prix, conformément au calcul ci-dessus.

4.1.2.6 Méthode de sélection

a) Pour être déclarée recevable, une soumission doit :

(i) respecter toutes les exigences de la demande de soumissions;
(ii) respecter tous les critères d'évaluation techniques obligatoires stipulés dans l'annexe J, Évaluation technique ; et,
(iii) obtenir la note minimale requise de 70 % pour les critères d'évaluation technique énoncés à l'annexe J, Critères d'évaluation des soumissions. Lesquels qui sont assujettis à une cote numérique.

Sous réserve du processus de conformité des soumissions par étapes, les soumissions ne répondant pas aux critères (i), (ii) ou (iii) seront déclarées non recevables.

b) Les soumissions seront classées selon la note la plus élevée à la plus faible et jusqu'à concurrence des trois soumissions recevables. Ces soumissions les mieux classés seront recommandées pour l'attribution d'un contrat. Pour chacun des trois soumissionnaires conformes les mieux classés, le Canada attribuera jusqu'à trois contrats d'une valeur de 200 000 $ CAN chacun, taxes applicables en sus. Les entrepreneurs devront exécuter les travaux définis à la phase 1 de l'annexe A, Énoncé des travaux.

c) Si un soumissionnaire retire sa soumission ou si sa soumission est écartée, le Canada peut offrir un contrat au soumissionnaire ayant obtenu la note la plus élevée suivante.

d) Dans l'éventualité où une égalité de points aurait une incidence sur le classement, le soumissionnaire conforme qui obtient la note technique la plus élevée sera recommandé pour l'attribution d'un contrat.

e) Les soumissionnaires devraient noter que l'attribution des contrats est assujettie au processus d'approbation interne du Canada, qui prévoit l'approbation obligatoire du financement selon le montant de tout contrat proposé. Même si un soumissionnaire a été recommandé pour l'attribution d'un contrat, un contrat sera attribué uniquement si l'approbation interne est obtenue conformément aux politiques internes du Canada. Si l'approbation n'est pas obtenue, aucun contrat ne sera attribué.

4.2 Droits du Canada

Le Canada se réserve le droit :

a) de rejeter l'une quelconque ou la totalité des soumissions reçues en réponse à la présente demande de propositions;

b) d'entreprendre des négociations avec les soumissionnaires sur n'importe quel aspect de leur soumission;

c) d'accepter une proposition en totalité ou en partie, sans négociation;

d) d'annuler l'appel d'offres à n'importe quel moment;

e) d'émettre de nouveau la demande de soumissions;

f) si aucune soumission recevable n'est reçue et que le besoin n'est pas modifié substantiellement, de publier de nouveau la demande de soumissions en invitant uniquement les soumissionnaires qui ont soumissionné à soumissionner de nouveau dans un délai indiqué par le Canada;

g) de négocier avec le seul soumissionnaire qui a déposé une proposition conforme pour s'assurer que le Canada profitera du meilleur rapport qualité-prix.

4.3 Rejet d'une soumission

a) Motifs de rejet. Le Canada peut rejeter une soumission lorsque le soumissionnaire est en faillite, lorsque ses activités sont suspendues pendant une longue période ou lorsque le soumissionnaire, un employé ou un sous-traitant proposé dans le cadre de la soumission :

(i) fait l'objet d'une mesure corrective du rendement des fournisseurs en vertu de la Politique sur les mesures correctives du rendement des fournisseurs, qui rend le soumissionnaire, l'employé ou le sous-traitant inadmissible à soumissionner pour le besoin;

(ii) est accusé de fraude, de corruption, d'assertion frauduleuse ou n'a pas respecté les lois protégeant les personnes contre toute forme de discrimination;

(iii) s'est conduit de façon répréhensible lors d'interactions actuelles ou antérieures avec le gouvernement du Canada;

(iv) a été suspendu ou que son marché a été résilié par le Canada pour inexécution à l'égard d'un contrat;

(v) a exécuté d'autres marchés d'une manière suffisamment médiocre pour qu'on le considère comme incapable de répondre au besoin faisant l'objet de la proposition.

b) Avis de rejet pour suspension ou résiliation. Dans le cas où le Canada a l'intention de rejeter une soumission en raison de la suspension, de la résiliation ou de l'exécution suffisamment médiocre d'un autre marché, l'autorité contractante préviendra le soumissionnaire et lui donnera 10 jours pour faire valoir son point de vue, avant de prendre une décision définitive quant au rejet de la soumission.

c) Plusieurs soumissions reçues d'un même soumissionnaire ou d'une coentreprise. Le Canada se réserve le droit de procéder à un examen approfondi, en particulier lorsque plusieurs soumissions provenant d'un seul soumissionnaire ou d'une coentreprise sont reçues en réponse à une demande de soumissions. Le Canada se réserve le droit de rejeter une partie ou la totalité des soumissions présentées par un même soumissionnaire ou une coentreprise si leur inclusion :
(i) dans l'évaluation a pour effet de porter atteinte à l'intégrité et à l'équité du processus;
(ii) dans le processus d'approvisionnement fausserait l'évaluation relative à la demande de soumissions ou n'offrirait pas une bonne valeur au Canada.

4.4 Procédures d'évaluation des capacités et de la convivialité

a) **Séances de mobilisation pour le développement de prototype :** Après l'évaluation des soumissions et l'attribution d'un maximum de trois contrats de travail pour l'élaboration d'un prototype de solution conformément à la phase 1 - Prototype de solution de l'annexe A – Énoncé des travaux et aux critères de l'ECC décrits à l'appendice A de l'annexe A – Énoncé des travaux, le Canada interagira avec les entrepreneurs pour l'élaboration de leur prototype

de solution en organisant des séances de mobilisation des entrepreneurs conformément aux procédures décrites à l'appendice A de l'annexe A – Énoncé des travaux.

b) Lors des séances de mobilisation des entrepreneurs, le Canada fournira une rétroaction sur les prototypes au fur et à mesure de leur développement par les entrepreneurs. Ces interactions devraient permettre aux entrepreneurs de comprendre entièrement les exigences du Canada pour une solution innovante, avec une rétroaction de la part des utilisateurs au premier plan. Les séances seraient menées de la même manière pour tous les entrepreneurs afin de leur donner la même possibilité de faire des démonstrations et de demander une rétroaction ou des commentaires sur leur travail concernant le prototype. Cette approche souple exige que chaque entrepreneur participe aux séances de mobilisation tout au long du processus de développement du prototype.

c) Au cours de la phase de développement du prototype, toutes les demandes de renseignements des entrepreneurs doivent être soumises par écrit à l'autorité contractante pour que le Canada y réponde. Les demandes de renseignements techniques à caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque élément visé. Les éléments affichant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf si le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Le Canada peut modifier les questions ou peut demander à l'entrepreneur de le faire afin d'en éliminer le caractère exclusif et permettre la transmission des réponses à tous les entrepreneurs. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les entrepreneurs.

d) Évaluation des capacités et de la convivialité (ÉCC) **:** Une évaluation des capacités et de la convivialité (ECC) sera menée par le Canada à la suite de la réception des prototypes de solution soumis par les entrepreneurs. L'ÉCC sera effectuée en conformité avec la Phase 1- Prototype de Solution de l'Annexe A - Énoncé de travaux et les critères de l'ÉCC décrits dans l'Appendice A de l'Annexe A - Énoncé de travaux.

e) Les entrepreneurs devront soumettre tous les produits livrables du contrat pour les travaux de la phase 1, y compris un prototype de solution d'ECC, dans le format et à la date spécifiés dans le contrat pour l'évaluation du Canada en fonction des critères d'ECC décrits à l'appendice A de l'annexe A – Énoncé des travaux.

f) La solution de prototype de l'entrepreneur visée par l'ECC sera évaluée en fonction des critères cotés de l'ECC. Les critères cotés de l'ECC seront notés, et la somme des notes pour chaque catégorie sera calculée d'après les critères d'évaluation et les points maximums énumérés dans chaque catégorie de l'appendice A à l'annexe A – Énoncé des travaux.

g) La note d'évaluation globale de l'ECC sera calculée selon la note combinée la plus élevée pour le mérite technique, le prix et l'ECC.

h) Demandes de précisions ou de renseignements supplémentaires : Le Canada se réserve le droit de demander des éclaircissements ou au besoin des renseignements supplémentaires à l'entrepreneur pour vérifier tout ou une partie des renseignements fournis par l'entrepreneur ou pour compléter l'évaluation du Canada de la solution proposée par l'entrepreneur. L'entrepreneur doit fournir les renseignements nécessaires demandés par le Canada dans les 24 heures (ou dans un délai plus long si l'autorité contractante le précise par écrit). Si l'entrepreneur ne répond pas dans le délai prescrit, la solution de l'entrepreneur pourrait ne pas être prise en considération par le Canada. Si l'entrepreneur a besoin de plus de temps, l'autorité contractante peut accorder une prolongation à sa seule discrétion.

i) Fondement de la décision du Canada d'exercer l'option de solution de phase 2

La solution de prototype la mieux classé sera déterminée en fonction du fait que l'entrepreneur a satisfait à toutes les exigences de la phase 1 -Solution de prototype du contrat, ainsi que la

livraison de tous les produits livrables requis et l'obtention du résultat combiné la plus élevé en matière de mérite technique, de prix et de l'ÉCC. Une pondération de 10 % sera attribuée à la note d'évaluation technique. Une pondération de 30 % sera attribuée à la note d'évaluation financière. Une pondération de 60 % sera attribuée à la note CUA, conformément au tableau suivant :

Composantes de l'évaluation	Pondération globale
Note de l'évaluation technique*	10%
Note de l'évaluation financière*	30%
Note de l'Évaluation des capacités et de la convivialité (ÉCC)	60%

**REMARQUE : Les notes d'évaluation technique et financière mentionnées dans le tableau ci-dessus sont les notes obtenues lors de la phase d'évaluation des soumissions sur la base desquelles le ou les contrats de développement d'un prototype de solution est (sont) attribué(s).*

(i) En cas d'égalité, la note de l'ÉCC sera utilisée pour classer les entrepreneurs de la note la plus élevée à la note la plus faible. S'il y a d'autres égalités, la note financière la plus basse sera utilisée pour classer l'entrepreneur.

(ii) Test de prototype sur plateforme pour l'entrepreneur le mieux classé d'après l'ECC:

a. Dans le cadre du test du prototype sur plateforme, le Canada peut, à sa seule discrétion tester la solution proposée par l'entrepreneur le mieux classé (identifiée après l'évaluation d'ECC) pour confirmer à la fois qu'elle fonctionnera et s'intégrera comme décrit dans l'environnement de la GRC et qu'elle répondra aux exigences de fonctionnalité technique décrites dans l'annexe A – Évaluation des capacités et de l'utilisabilité (ECC) de l'énoncé des travaux - Annexe A du contrat. Si requis par le Canada, le test du prototype sur plateforme aura lieu dans la région de la capitale nationale, dans un emplacement fourni par le Canada, qui permettra de recréer l'environnement technique décrit à la section 4.6 – Déploiement au sein de l'espace infonuagique de la GRC de l'annexe A – Énoncé des travaux. L'entrepreneur devra disposer d'une équipe de soutien personnel sur place pour aider la GRC dans l'installation et l'intégration.

b. Après avoir été informé par l'autorité contractante de la décision de mener un Test de prototype sur plateforme, le soumissionnaire aura un maximum de dix (10) jours ouvrables pour commencer à préparer le déplacement du prototype vers l'environnement désigné de la GRC. Pendant ce temps de préparation :

i. l'entrepreneur doit fournir toute la documentation et les instructions pour l'installation et l'intégration du prototype dans l'espace infonuagique Protégé B de la GRC;
ii. l'entrepreneur doit déterminer tous les outils nécessaires qui feront partie de l'installation et de l'intégration;

iii. l'entrepreneur doit désigner le ou les représentants de l'équipe de soutien qui assisteront la GRC dans l'installation et l'intégration sur le site de la GRC;
iv. l'entrepreneur doit emballer et livrer le prototype de manière à ce que la GRC puisse commencer l'installation à une date précise.

c. Le Canada consignera les résultats du test de prototype sur plateforme. Si le Canada juge que la solution proposée ne satisfait pas à une exigence obligatoire du test de prototype sur plateforme, le soumissionnaire ne réussira pas le test de prototype sur plateforme et sera rejeté. Si l'entrepreneur le mieux classé a échoué au test de prototype sur plateforme, le Canada peut, à sa discrétion, demander à l'entrepreneur classé en deuxième position (choisi après l'évaluation de l'ECC) d'effectuer un test de prototype sur plateforme de la solution qu'il propose.

d. Dans le cadre du test de prototype sur plateforme, l'entrepreneur accorde au Canada une licence restreinte d'utilisation de sa solution logicielle proposée aux fins d'essai et d'évaluation.

e. Si, au cours de l'installation initiale du logiciel pour le test de prototype sur plateforme, l'entrepreneur découvre que des fichiers pour les composantes logicielles précisées dans la soumission technique sont manquants ou corrompus, il doit cesser le processus d'installation et aviser l'autorité contractante. Si l'autorité contractante détermine que les fichiers manquants ou corrompus font partie des composantes précisées dans la soumission technique, le soumissionnaire peut obtenir la permission de présenter à l'autorité contractante les fichiers manquants ou les fichiers qui remplacent les fichiers corrompus sur un support électronique ou un site Web où les fichiers peuvent être téléchargés. Ces fichiers doivent avoir été rendus accessibles publiquement dans le commerce 10 jours civils avant la date prévue pour le test de prototype sur plateforme. À la réception des fichiers sous forme électronique ou téléchargés d'un site Web d'entreprise, l'autorité contractante vérifiera que (i) les fichiers ont été rendus accessibles publiquement dans le commerce 10 jours civils avant la date prévue pour le test de prototype sur plateforme; (ii) les fichiers ne comprennent pas de nouvelles éditions ou versions du logiciel; (iii) les fichiers appartiennent à des composantes logicielles précisées dans la soumission technique; et (iv) le logiciel n'aura pas à être recompilé pour que les fichiers puissent être utilisés. L'autorité contractante décidera, à sa seule discrétion, si les fichiers supplémentaires peuvent être installés pour le test de prototype sur plateforme. En aucun cas les fichiers nécessaires pour corriger des défauts de programmation ou de code du logiciel ne seront permis. Ce processus ne peut être utilisé qu'une seule fois, et ce, seulement au cours de l'installation initiale du logiciel pour le test de prototype sur plateforme.

(iii) Une fois toutes les évaluations terminées, le Canada exercera, à sa seule discrétion, l'option irrévocable de sélectionner un entrepreneur pour exécuter la totalité ou une partie des travaux visés à l'article 3. Phase 2 – Solution de l'annexe A – Énoncé des travaux. Le Canada peut également, à sa discrétion, exercer son option irrévocable auprès d'autres entrepreneurs qui ont pris part à l'ECC pour la totalité ou une partie des travaux, s'il est déterminé que cela répondrait le mieux aux besoins du Canada. .

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

Les soumissionnaires doivent fournir les attestations et les renseignements supplémentaires exigés pour qu'un contrat leur soit attribué.

Les attestations que les soumissionnaires remettent au gouvernement du Canada peuvent être vérifiées à tout moment par ce dernier. À moins d'indication contraire, le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur s'il est établi qu'une attestation du soumissionnaire est fausse, sciemment ou non, que ce soit pendant la période d'évaluation des soumissions ou pendant la durée du contrat.

L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. À défaut de répondre et de coopérer à toute demande ou exigence imposée par l'autorité contractante, la soumission sera déclarée non recevable, ou constituera un manquement aux termes du contrat.

5.1 Attestations à fournir avec la proposition

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

a) **Dispositions relatives à l'intégrité – Déclaration de condamnation à une infraction**
Conformément aux Dispositions relatives à l'intégrité des Instructions générales, tous les soumissionnaires doivent fournir avec leur proposition, **le cas échéant**, le formulaire de déclaration d'intégrité (formulaire 5) se trouvant sur le site Web des formulaires du régime d'intégrité (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html), afin que leur proposition soit prise en compte dans le cadre du processus d'approvisionnement.

b) **Ressources en services professionnels**

i. En soumettant une soumission, le soumissionnaire atteste que chaque personne proposée dans sa soumission sera, en cas de contrat subséquent, disponible pour exécuter les travaux requis par le représentant du Canada et au moment précisé dans la demande de soumissions ou convenu avec les représentants du Canada.

ii. En présentant une soumission, le soumissionnaire atteste que tous les renseignements fournis dans les curriculum vitæ et les documents justificatifs présentés avec sa soumission, en particulier les renseignements relatifs aux études, aux réalisations, à l'expérience et aux antécédents professionnels, ont été vérifiés par le soumissionnaire et sont exacts et authentiques. De plus, le soumissionnaire garantit que chaque personne proposée par le soumissionnaire pour le besoin est en mesure d'exécuter les travaux décrits dans le contrat subséquent.

iii. Si un soumissionnaire a proposé dans sa soumission une personne qui n'est pas un employé du soumissionnaire, le soumissionnaire atteste qu'il a la permission de cette personne de proposer ses services relativement aux travaux à exécuter et de présenter son curriculum vitæ au Canada. Le soumissionnaire doit, sur demande de l'autorité contractante, fournir une confirmation écrite, signée par la personne, de la permission donnée au soumissionnaire et de sa disponibilité. Si la demande n'est pas satisfaite, la soumission peut être déclarée non recevable.

c) **Attestation de l'éditeur de logiciels, autorisation de l'éditeur de logiciels et attestation du contributeur de logiciels**

i. Si le soumissionnaire est le concepteur de tout élément des logiciels privés proposés, le Canada exige que le soumissionnaire confirme, par écrit, qu'il est le concepteur de logiciels. Les soumissionnaires doivent utiliser le formulaire d'attestation du concepteur de logiciels joint à la demande de soumissions. Bien qu'il soit nécessaire de fournir tous les renseignements demandés dans le formulaire d'attestation du concepteur de logiciels, l'utilisation de ce formulaire n'est pas obligatoire. Dans le cas des soumissionnaires qui utilisent un autre formulaire, il appartient entièrement au Canada, à sa seule discrétion, de déterminer si tous les renseignements exigés ont été fournis. Toute modification apportée aux énoncés du formulaire pourrait rendre la soumission non recevable.

ii. Tout soumissionnaire qui n'est pas le concepteur de tous les produits logiciels proposés dans le cadre de sa soumission doit présenter une preuve de l'autorisation du concepteur de logiciels, qui doit être signée par ce dernier (et non par le soumissionnaire). Aucun contrat ne sera attribué à un soumissionnaire qui n'est pas le concepteur de tous les logiciels privés proposés au Canada, à moins qu'une preuve de l'autorisation de ce dernier n'ait été fournie au Canada. Si les logiciels privés proposés par le soumissionnaire proviennent de plusieurs concepteurs de logiciels, une autorisation est exigée de chaque concepteur de logiciels. On demande aux soumissionnaires d'utiliser le formulaire d'autorisation du concepteur de logiciels joint à la demande de soumissions. Bien qu'il soit nécessaire de fournir tous les renseignements demandés dans le formulaire d'attestation du concepteur de logiciels, l'utilisation de ce formulaire n'est pas obligatoire. Quant aux soumissionnaires et aux concepteurs de logiciels qui utilisent un autre formulaire, il revient à la seule discrétion du Canada de déterminer si tous les renseignements exigés ont été fournis. Toute modification apportée aux énoncés du formulaire pourrait rendre la soumission non recevable.

iii. Dans le cadre de la présente demande de soumissions, « concepteur de logiciels » désigne le propriétaire de tout produit logiciel compris dans la soumission qui a le droit d'octroyer une licence (et d'autoriser d'autres personnes à octroyer une licence ou une sous-licence) pour ses produits logiciels.

iv. Les documents d'attestation suivants sont exigés dans la soumission :

Formulaire 2, Lettre d'attestation du fournisseur de services infonuagiques
Formulaire 3, Attestation du concepteur de logiciel-service
Formulaire 4, Autorisation du concepteur de logiciel-service

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

Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être remplis et fournis avec la soumission, mais ils peuvent être fournis plus tard. Si l'une des attestations exigées ou l'un des renseignements supplémentaires requis n'est pas fourni conformément aux exigences, l'autorité contractante informera le soumissionnaire du délai dont il dispose pour le faire. Si le soumissionnaire ne fournit pas les attestations et les renseignements supplémentaires énoncés ci-dessous dans le délai établi, sa soumission sera déclarée non recevable.

5.2.1 Processus d'intégrité de la chaîne d'approvisionnement

(1) Au cours du processus de demande de propositions, de la période du contrat et de toute période d'option qui en découle, l'autorité responsable de la sécurité de la chaîne d'approvisionnement désignée par le Canada peut évaluer l'l'information sur la sécurité de la chaîne d'approvisionnement (ISCA) du soumissionnaire en fonction de son mandat de

sécurité nationale visant à protéger l'infrastructure de TI du Canada ainsi qu'à évaluer les menaces, les risques et les vulnérabilités.

(2) Le Canada évaluera si, à son avis, la chaîne d'approvisionnement du soumissionnaire crée la possibilité que sa chaîne d'approvisionnement ou sa solution proposée pourrait compromettre ou servir à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, ou représenter une menace pour la sécurité nationale du Canada, selon le Processus d'intégrité de la chaîne d'approvisionnement (annexe F).

(3) La condition préalable à toute attribution de contrat est qu'un soumissionnaire obtienne un résultat satisfaisant à l'évaluation de l'intégrité de la chaîne d'approvisionnement effectuée par l'autorité responsable de la sécurité.

5.2.2 Évaluation de la TI

La condition préalable à toute attribution de contrat est qu'un soumissionnaire remplisse le programme d'évaluation des TI du Centre canadien pour la cybersécurité (CCC).

5.3 Dispositions relatives à l'intégrité – Documents obligatoires

En vertu de la section intitulée Renseignements à fournir lors d'une soumission, de la passation d'un contrat ou de la conclusion d'un contrat immobilier de la *Politique d'inadmissibilité et de suspension* (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html), l'entrepreneur doit présenter la documentation exigée, s'il y a lieu, sinon sa soumission sera rejetée.

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

En présentant une soumission, le soumissionnaire atteste que ni lui ni un membre de la coentreprise, si le soumissionnaire est une coentreprise, ne sont nommés dans la « Liste d'admissibilité limitée à soumissionner au Programme de contrats fédéraux » qui figure au bas de la page du site Web du Programme du travail d'Emploi et Développement social Canada (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html).

Le gouvernement du Canada aura le droit de déclarer une soumission non recevable si le soumissionnaire ou tout membre de la coentreprise, si le soumissionnaire est une coentreprise, figure dans la liste d'admissibilité limitée à soumissionner au Programme de contrats fédéraux au moment de l'attribution du contrat.

Le Canada aura aussi le droit de résilier le contrat pour manquement si l'entrepreneur, ou tout membre de la coentreprise si l'entrepreneur est une coentreprise, figure sur la « Liste d'admissibilité limitée à soumissionner au Programme de contrats fédéraux » pendant la durée du contrat.

Le soumissionnaire doit fournir à l'autorité contractante le formulaire 7 dûment rempli intitulé Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, avant l'attribution du contrat. Si le soumissionnaire est une coentreprise, il doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, dûment remplie, pour chaque membre de la coentreprise.

5.5 Soumission unique – Justification du prix

Si votre soumission est la seule reçue, le support des prix doit être remis avec l'offre, conformément au *Règlement sur les marchés de l'État*. L'une ou l'autre des justifications suivantes est acceptable :

a) la liste de prix publiée la plus récente, indiquant l'escompte, en pourcentage, offert au Canada; ou

b) des copies des factures payées se rapportant à la prestation de services semblables à d'autres clients ou à la vente d'articles semblables (même quantité et même qualité) à d'autres clients, ou à ces deux éléments; ou

c) une ventilation des prix indiquant le coût de la main-d'œuvre directe, des matières directes et des articles achetés, les coûts indirects associés aux services techniques et aux installations, les coûts indirects généraux et administratifs, les coûts de transport etc., et le bénéfice; ou

d) des attestations des prix ou des tarifs; ou

e) toute autre pièce justificative demandée par le Canada.

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ ET EXIGENCES FINANCIÈRES

Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées :

6.1 Fournisseurs canadiens

a) Le contractant ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ B, délivrées par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

b) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une COTE DE FIABILITÉ valide, délivrée ou approuvée par la DSIC/SPAC.

c) L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements PROTÉGÉS tant que la DSIC de TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée ou approuvée, ces tâches pourront être exécutées au niveau PROTÉGÉ B (y compris un lien électronique au niveau PROTÉGÉ B).

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

e) L'entrepreneur ou l'offrant devra respecter les dispositions:

(i) de la liste de vérification des exigences en matière de sécurité et la directive de sécurité (s'il y a lieu), ci-jointes à l'annexe C;
(ii) du Manuel de la sécurité industrielle (plus récente édition).

6.2 Fournisseur étranger

L'administration désignée en matière de sécurité (ADS canadienne) pour les questions industrielles au Canada est le Secteur de la sécurité industrielle (SSI), Travaux publics et Services gouvernementaux Canada (TPSGC), administré par la Direction de la sécurité industrielle internationale (DSII). L'ADS canadienne est chargée d'évaluer la conformité des soumissionnaires avec les exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux soumissionnaires étrangers destinataires qui sont constitués en personne morale ou autorisés à faire des affaires dans un État autre que le Canada et à livrer ou exécuter la solution, en plus des exigences relatives à la vie privée et à la sécurité. Ces exigences en matière de sécurité s'ajoutent aux exigences déjà déterminées ci-dessous dans la section Protection et sécurité des données emmagasinées dans des bases de données.

a) Le soumissionnaire étranger destinataire doit provenir d'un pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Union européenne (UE) ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité industrielle. Le Programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatérale ou multinationale industrielle avec les pays mentionnés au site suivant de TPSGC : https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

b) Le soumissionnaire étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence, comme il est indiqué à la Partie 7 – Clauses du contrat subséquent.

c) Le soumissionnaire étranger destinataire doit être inscrit auprès de l'autorité gouvernementale compétente chargée de superviser la protection des renseignements personnels des pays dans lesquels il a été constitué ou il est en activité et autorisé à exercer des activités commerciales ou à exploiter une entreprise, comme il est indiqué à la partie 7 - Clauses du contrat subséquent, 7.5(b) Exigences en matière de sécurité pour les fournisseurs étrangers.

d) Le soumissionnaire étranger destinataire doit fournir l'assurance qu'il peut recevoir et stocker des renseignements personnels ou biens de niveau PROTÉGÉ B AU CANADA sur son site ou sur les lieux, comme il est indiqué à la Partie 7 – Clauses du contrat subséquent et dans les exigences relatives à la sécurité des TI.

e) Le lieu proposé par le soumissionnaire étranger destinataire pour l'exécution des travaux doit satisfaire aux exigences relatives à la sécurité, comme il est indiqué dans la partie 7 et dans les exigences relatives à la sécurité des TI.

f) Le soumissionnaire étranger destinataire doit fournir l'adresse du ou des lieux proposés pour la réalisation des travaux et pour la protection des documents.

g) Les personnes proposées par le soumissionnaire étranger destinataire retenu qui doivent accéder à des renseignements personnels ou des biens PROTÉGÉ B AU CANADA ou encore à des sites de travail restreints doivent CHACUNE détenir une vérification du casier judiciaire valide, avec des résultats favorables, d'un organisme gouvernemental reconnu ou d'une organisation du secteur privé reconnue de son pays, ainsi qu'une vérification des antécédents, validée par l'ADS canadienne.

h) Les personnes proposées par le soumissionnaire étranger destinataire retenu ne doivent pas entamer les travaux avant que toutes les exigences relatives à la sécurité aient été respectées.

i) Si le soumissionnaire est une coentreprise, chacun des membres de celle-ci doit respecter les exigences relatives à la sécurité et à la protection de la vie privé.

j) Les soumissionnaires étrangers destinataires doivent fournir une preuve indiquant que toutes les bases de données, y compris la base de données des sauvegardes utilisée par les organisations pour fournir les services décrits dans l'EDT qui renferment des renseignements personnels PROTÉGÉ B AU CANADA relativement aux travaux se trouvent au Canada.

k) Le soumissionnaire étranger destinataire reconnu NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker dans un système informatique des renseignements personnels et des biens PROTÉGÉ B AU CANADA avant d'avoir obtenu l'autorisation de l'ADS canadienne.

l) La soumission devrait clairement indiquer les travaux que le soumissionnaire étranger destinataire prévoit confier en sous-traitance. Tous les contrats de sous-traitance dans lesquels il est prévu que le sous-traitant aura accès à des renseignements personnels PROTÉGÉS AU CANADA sont assujettis à l'approbation du Canada. La description des contrats de sous-traitance doit indiquer comment le soumissionnaire étranger destinataire assurera le respect des exigences, des modalités, des conditions et des clauses du contrat de sous-traitance.

m) Si un soumissionnaire étranger destinataire est choisi comme entrepreneur dans le cadre de ce contrat, des clauses de sécurité propres à son pays seront établies et mises en œuvre par l'ADS canadienne; ces clauses seront fournies à l'autorité contractante du gouvernement du Canada, afin de respecter les dispositions de sécurité.

6.3 Capacité financière

La clause A9033T (2012-07-16), Capacité financière, du Guide des CCUA s'applique. Cependant, le paragraphe 3 est supprimé et est remplacé par : « Si le soumissionnaire est une filiale d'une autre entreprise, chaque société mère, y compris la société mère ultime, devra fournir l'information financière demandée par l'autorité contractante en 1(a) à (f). La fourniture des renseignements financiers de la société mère ne répond pas à elle seule à l'exigence selon laquelle le soumissionnaire doit fournir ses renseignements financiers; toutefois, si le soumissionnaire est une

filiale d'une autre entreprise, et si, dans le cours normal des affaires, les renseignements financiers ne sont pas générés distinctement pour la filiale, les renseignements financiers de la société mère doivent donc être fournis. Si le Canada juge que le soumissionnaire ne possède pas la capacité financière nécessaire, mais que la société mère la possède, ou si le Canada ne peut évaluer la capacité financière du soumissionnaire puisqu'elle fait partie intégrante de celle de la société mère, le Canada peut, à sa seule discrétion, attribuer le contrat au soumissionnaire sous réserve qu'au moins une des sociétés mères fournisse une garantie au Canada ».

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

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

Le présent contrat est conclu le [DATE DU CONTRAT] entre [NOM DE L'ENTREPRENEUR] (« l'entrepreneur ») et [ENTITÉ DU GOUVERNEMENT DU CANADA] (« Canada »).

7.1 Besoin

a) L'entrepreneur convient de fournir au client les travaux, les biens, les services et d'exécuter les travaux décrits dans le contrat (y compris l'Annexe A - Énoncé des travaux - EDT) conformément au contrat et aux prix indiqués dans celui-ci. Cela comprend au minimum :

Phase 1 de l'EDT : Tous les travaux et livrables associés à la phase 1 du prototype de solution, incluant la participation des entrepreneurs aux séances de mobilisation des entrepreneurs, et au processus de test du prototype sur la plateforme le cas échéant, et;

Phase 2 de l'EDT (s'il y a lieu) : Au fur et à mesure de l'autorisation, tous les travaux et produits livrables associés à la phase 2 de la solution complète :

Ce qui comprend, sans s'y limiter :

i. accorder une licence d'utilisation aux utilisateurs ou un accès aux utilisateurs ou les deux, selon le cas, pour utiliser la solution pour 100 utilisateurs pendant la phase 1 de la solution prototype de l'EDT, et jusqu'à 2 000 utilisateurs (y compris 500 utilisateurs simultanés) pour la phase 2 de la solution finale, s'il y a lieu ;

ii. effectuer tout travail nécessaire à la conception ou à l'élaboration de caractéristiques ou de fonctionnalités, et élaborer et mettre en œuvre tout composant logiciel commercial ou personnalisé pour la solution prototype et la solution complète, s'il y a lieu ;

iii. fournir toute application logicielle et tout composant liés à la solution requis pour accéder à la solution prototype et l'utiliser, ainsi qu'à la solution complète, le cas échéant, en ligne et dans l'environnement du client, le cas échéant, conformément au modèle de prestation de la solution de l'entrepreneur ;

iv. mettre en place et ajuster, le cas échéant, la solution prototype et la solution complète, le cas échéant, dans le Cloud et dans l'environnement du Client, conformément au modèle de prestation de la solution de l'entrepreneur ;

v. entretenir et mettre à jour la solution complète, s'il y a lieu, tous les services de ressources informatiques de la solution et de tous les composants sous la responsabilité de l'entrepreneur, conformément au modèle de prestation de la solution de l'entrepreneur ;

vi. gérer les incidents et les défectuosités de la solution complète, s'il y a lieu, survenant à tout composant de ressources informatiques de la solution sous la responsabilité de l'entrepreneur, conformément au modèle de prestation de la solution de l'entrepreneur; afin de garantir un fonctionnement optimal de la Solution aux niveaux de service applicables ;

vii. fournir la documentation d'exploitation, de formation et d'entretien la solution prototype et la solution complète, s'il y a lieu, conformément au modèle de prestation de la solution de l'entrepreneur ;

viii. fournir une garantie de 12 mois pour tout composant logiciel lié à la solution fonctionnant dans l'environnement du client, le cas échéant, conformément au modèle de prestation de la solution de l'entrepreneur ;

ix. fournir les plans, les rapports, les réunions, la conception, la modélisation, la gestion, la formation, les évaluations, l'expertise technique, la documentation et les services de soutien liés à l'élaboration, à la mise en œuvre, au déploiement et à la transition d'une solution sous licence ; et

x. fournir des services professionnels et des services de formation supplémentaires, à la demande du Canada, conformément au processus d'autorisation de tâches (AT) décrit aux présentes.

b) **Biens et services optionnels**

L'entrepreneur accorde au Canada le droit d'exercer les options irrévocables suivantes pour acquérir des biens et des services. Les options sont décrites en détail à l'annexe A – Énoncé des travaux et les prix sont indiqués à l'annexe B – Base de paiement. Toutes les options seront exercées par l'autorité contractante et seront confirmées par une modification au contrat. L'autorité contractante peut exercer toute option à tout moment avant l'expiration du contrat en envoyant un avis écrit à l'entrepreneur. Cela comprend au minimum :

i. option de mettre en œuvre et de livrer la solution complète conformément aux travaux de la phase 2 décrits à l'annexe A - Énoncé des travaux, y compris la fourniture de plans, de rapports, de réunions, de conception, de modélisation, de mise à l'essai, d'évaluations, d'expertise technique, de documentation et de services de soutien liés au développement, à la mise en œuvre, au déploiement et à la transition de la solution complète conformément au modèle de prestation de la solution de l'entrepreneur. L'entrepreneur convient qu'il sera payé conformément aux dispositions applicables énoncées à l'annexe B – Base de paiement ;

ii. option pour acquérir, à la seule discrétion du Canada, des licences d'utilisation supplémentaires ou des accès d'utilisateur supplémentaires, ou les deux, selon le cas, conformément à l'annexe A – Énoncé des travaux et au prix indiqué à l'annexe B – Base de paiement ;

iii. option pour acquérir, sur demande, au moyen d'une autorisation de tâches des services professionnels et de la formation conformément à l'annexe A, Énoncé des travaux, et aux prix indiqués à l'annexe B, Base de paiement ; et

iv. option pour acquérir, au fur et à mesure des besoins et au moyen d'une autorisation de tâches, des services de maintenance et de soutien de la solution (le cas échéant) ou des services d'hébergement et de soutien liés à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant), conformément à l'annexe A - Énoncé des travaux et aux prix indiqués à l'annexe B - Base de paiement.

L'autorité contractante exercera cette ou ces options, selon les mêmes termes et conditions et aux prix et taux indiqués à l'annexe B – Base de paiement. Toute option sera confirmée par une modification au contrat.

L'autorité contractante peut exercer une option à n'importe quel moment avant la date d'échéance du contrat en envoyant un avis écrit à l'entrepreneur.

c) **Client** : Aux termes du contrat, le « **Client** » est la Gendarmerie Royale du Canada. Toutefois, l'autorité contractante peut progressivement ajouter des clients, y compris tout ministère ou toute société d'État mentionnés dans la *Loi sur la gestion des finances publiques* (et ses modifications), et toute autre partie au nom de laquelle le ministère des Travaux publics et des Services gouvernementaux est autorisé à agir en vertu de l'article 16 de la Loi sur le ministère des Travaux publics et des Services gouvernementaux.

d) **Réorganisation :** La réorganisation ou la restructuration d'un client n'aura aucune incidence sur l'obligation de l'entrepreneur en ce qui a trait à l'exécution des travaux (et ne donnera pas lieu non plus au paiement d'honoraires supplémentaires). Le Canada peut désigner une autorité contractante ou technique de remplacement.

e) **Évolution et utilisation de la solution :** Bien que le(s) contrat(s) soit d'une durée précise, le Canada se réserve le droit de continuer de contracter et de tirer parti de cette solution aussi longtemps qu'il est logique pour le Canada de le faire. Le Canada s'attend également à ce que la solution évolue avec le temps et les technologies, y compris l'intégration de fonctionnalités ou de technologies qui ne font pas actuellement partie du besoin. Le Canada se réserve le droit de considérer ces fonctionnalités ou technologies évolutives comme faisant partie de la portée continue des travaux effectués en vertu du contrat, sous réserve des processus d'approbation internes du Canada. Le Canada se réserve le droit, à une date ultérieure et à sa seule discrétion, d'identifier la solution soit comme solution pluriministérielle, soit de la désigner comme norme pangouvernementale du gouvernement du Canada, si et quand le GC le détermine par l'entremise du Comité d'examen de l'architecture d'entreprise (CEAAE) du GC.

f) **Définitions et interprétations :** Les définitions et les interprétations sont incluses à l'annexe D – Définitions et interprétations.

g) **Licence concernant le matériel protégé par des droits d'auteur :** Dans cet article, le terme « matériel » comprend tout ce qui est développé ou créé par l'entrepreneur en vertu des travaux prévus au contrat, et qui est protégé par des droits d'auteur.

i. L'entrepreneur accorde au Canada une licence non exclusive, perpétuelle, irrévocable, de portée mondiale, entièrement payée et libre de redevances pour exercer tous les droits couverts par le droit d'auteur sur le matériel pour les fins du gouvernement. Le Canada peut employer des entrepreneurs indépendants dans l'exercice de sa licence stipulée dans cette clause.

ii. Les droits d'auteur sur la traduction du matériel faite par le Canada ou en son nom appartiendront au Canada. Le Canada accepte de reproduire l'avis du droit d'auteur de l'entrepreneur, s'il en est, sur toutes les copies du matériel et de reconnaître, sur toutes les copies des traductions du matériel faites par le Canada ou en son nom, que l'entrepreneur détient la propriété du droit d'auteur sur l'oeuvre originale.

iii. Aucune autre restriction que celles indiquées dans cet article ne s'applique à l'utilisation, par le Canada, des copies du matériel ou des versions traduites du matériel.

iv. À la demande du Canada, l'entrepreneur doit fournir au Canada, soit à l'achèvement des travaux soit à telle autre date que pourra indiquer le Canada, une renonciation écrite permanente aux droits moraux, dans une forme acceptable pour le Canada, de la part de chaque auteur qui a contribué au matériel. Si l'entrepreneur est un auteur du matériel, il renonce en permanence à ses droits moraux se rapportant au matériel.

h) **Conditions générales et conditions générales supplémentaires**

(i) Conditions générales

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

ii. Les conditions 2030 (2020-05-28), Conditions générales – besoins plus complexes de biens sont intégrées au contrat subséquent.

iii. Les conditions 2035 (2020-05-28), Conditions générales – services plus complexes de services sont intégrées au contrat subséquent.

(ii) Conditions générales supplémentaires

Les conditions générales supplémentaires ci-après sont intégrées au contrat subséquent :

i. 4003 (2010-08-16) Logiciels sous licence ;

ii. 4004 (2013-04-25) Services de maintenance et de soutien des logiciels sous licence ;

iii. 4006 (2010-08-16) L'entrepreneur détient les droits de propriété intellectuelle sur les renseignements originaux ; et

iv. 4008, (2008-12-12) Renseignements personnels.

7.2 Durée du contrat

a) **Période du contrat.** La période du contrat englobe toute la période au cours de laquelle l'entrepreneur est obligé de fournir les biens et les services et d'exécuter les travaux.

b) **Durée initiale :** Ce contrat commence à la date d'attribution du contrat pour une période de trois ans à compter de la date d'attribution du contrat. L'entrepreneur doit immédiatement commencer les travaux de l'annexe A - Énoncé des travaux après l'attribution du contrat par l'autorité contractante.

c) **Option de prolonger la durée du contrat :** L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat jusqu'à concurrence de huit périodes supplémentaires d'un an selon les mêmes modalités. L'entrepreneur convient que, pendant la période prolongée du contrat, il sera payé conformément aux dispositions applicables énoncées à l'annexe B – Base de paiement. Le Canada peut exercer la ou les options en tout temps avant l'expiration du contrat en envoyant un avis écrit à l'entrepreneur. L'option ne peut être exercée que par l'autorité contractante et sera confirmée, à des fins administratives seulement, par une modification au contrat.

d) **Dates de livraison :** L'entrepreneur doit fournir tous les produits livrables conformément aux dates de livraison indiquées à la phase 1 de l'annexe A – Énoncé des travaux. Si le Canada a exercé son option irrévocable pour que l'entrepreneur mette en œuvre et livre la solution complète, l'entrepreneur doit fournir tous les produits livrables conformément aux dates de livraison indiquées à la phase 2 de l'annexe A – Énoncé des travaux.

e) **Options supplémentaires**

(i) Option d'exercice de la phase 2 : L'entrepreneur accorde au Canada l'option irrévocable d'autoriser l'entrepreneur à exécuter les travaux décrits à l'article 3. « PHASE 2 –

SOLUTION COMPLÈTE » de l'annexe A – Énoncé des travaux. L'entrepreneur convient qu'il sera payé conformément aux dispositions applicables qui sont établies à l'annexe B – Base de paiement.

(ii) **Option d'achat de licences d'utilisateur supplémentaires ou d'accès d'utilisateur supplémentaires ou les deux, le cas échéant** : L'entrepreneur accorde au Canada l'option irrévocable d'acquérir des licences d'utilisation supplémentaires ou des accès d'utilisateur supplémentaires, ou les deux, le cas échéant, selon les mêmes modalités et conditions. L'entrepreneur convient qu'il sera payé conformément aux dispositions applicables énoncées à l'annexe B – Base de paiement ;

(iii) **Option d'acquisition de services professionnels** sur demande, conformément à l'annexe A – Énoncé des travaux et aux prix indiqués à l'annexe B – Base de paiement ;

(iv) **Option d'acquisition de services de formation** sur demande, tel qu'indiqué à l'annexe A, Énoncé des travaux, et aux prix indiqués à l'annexe B, Base de paiement ; et

(v) **Option pour acquérir, s'il y a lieu, services de maintenance et de soutien de la solution (le cas échéant) ou services d'hébergement et de soutien liés à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant)** sur demande, conformément à l'annexe A - Énoncé des travaux et aux prix indiqués à l'annexe B - Base de paiement.

7.3 Solution

a) **Solution logicielle.** L'entrepreneur doit livrer la solution conformément à la sous-section 7.1.

b) **Évolution de l'application logicielle; caractéristiques ou fonctions.** Le Canada reconnaît que la solution, l'application logicielle sous-jacente ou l'infrastructure associée peut évoluer pendant la durée du contrat. L'entrepreneur accepte de continuer de fournir les services à titre de solution disponible sur le marché, avec des fonctions ou des caractéristiques et à des conditions qui ne sont pas moins favorables qu'au moment de l'attribution du contrat.

c) **Améliorations et évolution de la solution.** Les parties reconnaissent que les technologies et les modèles opérationnels évoluent rapidement et qu'une solution fournie au début de la durée du contrat sera inévitablement différente d'une solution fournie à la fin de la durée du contrat, et que les méthodes par lesquelles tout périphérique potentiel est livré au Canada changeront ou évolueront probablement. Les parties reconnaissent aussi qu'au moment de conclure ce contrat, elles ne pourraient possiblement envisager tous les biens ou services qui peuvent être livrés dans le cadre du contrat, outre le fait qu'ils seront reliés à la livraison aux utilisateurs. Dans cette optique, les parties s'entendent sur ce qui suit :

(i) L'entrepreneur doit maintenir et améliorer continuellement la solution et l'infrastructure pendant toute la durée du contrat, sur une base commercialement raisonnable, et il doit offrir ces améliorations au Canada dans le cadre de l'abonnement ou de la licence du Canada, le cas échéant, sans rajustement de prix si ces améliorations sont également offertes à d'autres clients sans frais supplémentaires.

(ii) Si l'entrepreneur retire des fonctions de l'offre commerciale de la solution et offre ces fonctions dans de nouveaux ou d'autres services ou produits, l'entrepreneur doit continuer de fournir ces fonctions au Canada dans le cadre de l'abonnement ou de licence du Canada, le cas échéant, aux services, selon les modalités actuelles du contrat, que ces autres services ou produits contiennent ou non des fonctions nouvelles ou supplémentaires. L'entrepreneur n'est pas obligé de se conformer à ce paragraphe si la

solution acquise par le Canada est toujours offerte par l'entrepreneur parallèlement aux nouveaux services offerts à d'autres clients.

d) **Déclassement.** Si l'entrepreneur est incapable de fournir les services avec des caractéristiques et des fonctions qui ne sont pas moins favorables, l'entrepreneur donnera au Canada un avis écrit indiquant les circonstances et des options de rechange, en plus d'inclure expressément une réduction de prix. Si aucune option de rechange proposée n'est acceptable pour le Canada, l'entrepreneur consent à une résiliation du contrat et paie tous les coûts directs identifiables engagés par le Canada pour effectuer la migration et le stockage des données de client et pour acquérir des services de remplacement équivalents.

e) **Versions de mise à jour.** Pendant la période de soutien du logiciel, l'entrepreneur doit fournir au Canada toute les versions de maintenance, sous forme de code objet et sans frais. Toutes les versions de mise à jour feront partie de la solution et seront soumises aux conditions de licence du Canada se rapportant à la solution. sauf indication contraire dans le contrat, l'e Canada recevra au moins une version de mise à jour pendant toute période de maintenance de douze (12) mois.

7.4 Changements opérationnels à la solution

a) Le gouvernement du Canada est à la recherche d'une **solution** novatrice qui peut s'adapter et évoluer avec les progrès technologiques pendant toute la durée du contrat. La **solution** fournie par l'entrepreneur doit être extensible et adaptable pour exploiter les innovations technologiques futures que l'entrepreneur pourrait utiliser pour mettre à niveau son logiciel sous licence. L'entrepreneur sera tenu de fournir gratuitement au gouvernement du Canada toutes les mises à niveau technologiques de la **solution** quand :

(i) la mise à niveau a été effectuée sur son logiciel sous licence;
(ii) la mise à niveau a été remise gratuitement aux autres clients de l'entrepreneur.

b) Le gouvernement du Canada exige également que l'entrepreneur veille à ce que la **solution** demeure compatible avec toutes les versions futures d'iOS, d'Android et des navigateurs Web suivants :

- Internet Explorer
- Google Chrome
- Firefox
- Safari

c) Le gouvernement du Canada a besoin que la solution demeure conforme aux normes de la Boîte à outils de l'expérience Web (BOEW) et des Règles pour l'accessibilité des contenus Web (WCAG), telles qu'elles sont définies dans l'énoncé des travaux, pendant toute la durée du contrat.

d) **Maintenance continue du code de logiciel :** L'entrepreneur doit continuer d'assurer la maintenance de la solution (c.-à-d. de la version ou de l'« édition » acceptée au départ et faisant l'objet des licences accordées en vertu du contrat). Par souci de clarté, l'entrepreneur ou l'éditeur de logiciel doit continuer à développer les codes du logiciel des composantes de la **solution** afin de maintenir et d'améliorer la fonctionnalité de celle-ci et de corriger les erreurs de logiciel pendant au moins 1 an après la date d'acceptation de la **solution**, conformément aux critères d'acceptation de l'annexe A – Énoncé des travaux. Si, après cette période, l'entrepreneur ou l'éditeur de logiciels décide de cesser la maintenance de la version ou de l'« édition » en cours de toute composante de la **solution** et décide plutôt d'offrir des mises à jour de toute composante du logiciel sous licence dans le cadre de la maintenance, il doit en informer le Canada par écrit au moins douze (12) mois avant cette cessation.

7.5 Maintenance et soutien de la solution

a) L'entrepreneur doit héberger, maintenir et prendre en charge la solution continuellement.

b) **Soutien de la solution.** Les services de soutien de la solution comprennent les services de dépannage téléphoniques et de soutien Web ci-dessous :

i. **Service téléphonique de soutien technique** : L'entrepreneur doit assurer un service téléphonique de soutien technique sans frais au (INSÉRER À L'ATTRIBUTION DU CONTRAT), en anglais et en français, de 8 h à 17 h (heure normale de l'Est), du lundi au vendredi, à l'exclusion des jours fériés qu'observe le gouvernement fédéral dans la province d'où provient l'appel. L'entrepreneur doit répondre aux appels ou retourner les appels dans les 60 minutes suivant leur réception. Le service de dépannage téléphonique de l'entrepreneur doit être assuré par des employés compétents, capables de répondre aux questions du client et des utilisateurs et, dans la mesure possible, de résoudre les problèmes par téléphone et d'offrir des conseils concernant les problèmes de configuration liés aux logiciels sous licence.

ii. **Soutien Web** : L'entrepreneur doit fournir au Canada un soutien technique par l'entremise d'un service de soutien Web, qui comprendra, au minimum, une foire aux questions et des routines de diagnostic, des outils de soutien et des services en ligne. Le site Web de l'entrepreneur doit offrir un soutien en anglais. Le Canada doit pouvoir accéder au site Web de l'entrepreneur 24 heures sur 24, 365 jours par année, et ce site doit être disponible 99 % du temps. L'adresse du site Web de l'entrepreneur est (INSÉRER À L'ATTRIBUTION DU CONTRAT).

c) **Services de correction d'erreurs de logiciel**

i. Le Canada peut rapporter à l'entrepreneur tout fonctionnement de la solution sous licence qui n'est pas conforme à la documentation de la solution ou, s'il y a lieu, aux spécifications pendant la période de soutien du logiciel. Le Canada peut signaler ces défaillances par écrit, par téléphone ou par un autre moyen de télécommunication. À la réception d'un avis de défaillance du Canada, sauf disposition contraire dans le contrat, l'entrepreneur doit employer tous les moyens raisonnables pour remettre au Canada, dans les délais prévus dans les sous-sections ii et iii, une correction de l'erreur de logiciel qui a causé la défaillance. Toute correction de ce genre devra assurer la conformité de la solution avec la documentation du logiciel ou, s'il y a lieu, les spécifications pendant la période de soutien du logiciel. L'entrepreneur doit faire tout ce qui est raisonnablement possible pour apporter des corrections permanentes à toutes les erreurs du logiciel et il garantit que la solution continuera de satisfaire les critères fonctionnels et de rendement établis dans les spécifications. Toutes les corrections apportées aux erreurs de logiciel feront partie de la solution et seront soumises aux conditions de la licence du Canada se rapportant à la solution.

ii. Sauf indication contraire dans le contrat, l'entrepreneur doit réagir à une erreur logicielle d'après la gravité de l'erreur, selon ce qui est exposé en détail dans la sous-section iii. Le Canada déterminera raisonnablement la gravité de l'erreur et la communiquera à l'entrepreneur, selon les définitions indiquées ci-dessous:

« Degré 1 » :

Défaillance d'un programme sous licence qui empêche l'utilisateur d'employer ledit programme, ce qui a des répercussions importantes pour ses objectifs

« Degré 2 » :

Défaillance d'un programme sous licence qui en restreint considérablement l'exploitation par l'utilisateur

« Degré 3 » :

Capacité d'utiliser seulement certaines fonctions d'un programme qui ne sont pas essentielles pour l'ensemble des opérations de l'utilisateur.

« Degré 4 » :

Le problème a été contourné ou corrigé temporairement et ne nuit pas aux opérations de l'utilisateur.

iii. Sauf disposition contraire figurant au contrat, l'entrepreneur doit déployer tous les efforts raisonnables pour corriger les erreurs de logiciel dans les délais indiqués ci-dessous.

« Degré 1 » :

dans les vingt-quatre (24) heures de l'avis donné par le Canada;

« Degré 2 » :

dans les soixante-douze (72) heures de l'avis donné par le Canada;

« Degré 3 » :

dans les quatorze (14) jours de l'avis donné par le Canada;

« Degré 4 » :

dans les quatre-vingt-dix (90) jours de l'avis donné par le Canada.

iv. Si une erreur logique est rapportée à l'entrepreneur, le Canada devra lui fournir un accès raisonnable au système informatique sur lequel le logiciel sous licence est installé et devra fournir l'information pertinente que l'entrepreneur demandera, y compris des échantillons de sorties et d'autres informations diagnostiques afin de lui permettre de résoudre le problème rapidement.

7.6 Utilisation des données du Canada par l'entrepreneur

a) Un accès aux données du Canada est accordé à l'entrepreneur, pour la durée du contrat, de manière unique et exclusive, afin de les utiliser pour fournir la **solution** aux utilisateurs, y compris une licence lui permettant de recueillir, de traiter, de stocker, de générer et d'afficher les données du Canada, uniquement dans la mesure requise pour fournir les services.

b) L'entrepreneur doit :

(i) conserver les données du Canada de manière strictement confidentielle, en adoptant le degré de diligence nécessaire et conforme aux obligations décrites dans la présente entente et les lois applicables afin d'éviter la perte ou l'accès, l'utilisation ou la divulgation non autorisés;

(ii) utiliser et divulguer les données du Canada uniquement et exclusivement afin de fournir le service, et ce, conformément au contrat et aux lois applicables;

(iii) s'abstenir d'utiliser, de vendre, de louer, de transférer, de distribuer ou de divulguer ou de rendre disponibles les données du Canada à ses propres fins ou au profit de toute personne autre que le Canada, sans obtenir le consentement préalable écrit de celui-ci.

(iv) fournir au Canada un accès complet à toutes les données de la solution

L'entrepreneur, ses sous-traitants et leurs employés respectifs doivent s'identifier auprès des individus desquels ils recueillent des renseignements personnels et leur donner le moyen de

vérifier qu'ils sont autorisés à recueillir les renseignements personnels en vertu d'un contrat passé avec le Canada.

Si l'autorité technique l'exige, l'entrepreneur doit élaborer un formulaire de demande de consentement à utiliser lors de la cueillette de renseignements personnels, ou un texte dans le cas de collecte de renseignements personnels par téléphone. L´entrepreneur ne peut utiliser le formulaire ou le texte sans avoir obtenu l´approbation écrite préalable de l´autorité contractante. Il doit aussi obtenir le consentement de l´autorité contractante avant de modifier le formulaire ou le texte.

Si, au moment de la collecte de renseignements personnels auprès d'un individu, l'entrepreneur soupçonne que cet individu n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, l'entrepreneur doit demander des directives à l'autorité technique.

7.7 Services

a) **Services de solution**

(i) L'entrepreneur fournira tous les services dont le Canada a besoin pour accéder à la solution et l'utiliser, selon ce qui est précisé à l'annexe A – Énoncé des travaux.

(ii) **Autorisations.** L'entrepreneur déclare et certifie qu'il possède ou a obtenu, et maintiendra pendant toute la durée du contrat, toutes les autorisations nécessaires, notamment les droits de propriété intellectuelle requis pour fournir les services d'après les modalités du contrat.

(iii) **Indemnisation.** L'entrepreneur accepte de tenir le Canada indemne de toute perte et de toute dépense (y compris les frais juridiques) découlant d'une demande concernant une violation de la propriété intellectuelle présentée par un tiers d'après l'utilisation de la solution par le Canada.

(iv) **Accessibilité :** L'entrepreneur doit s'assurer que la solution n'entrave pas au respecter des normes, tel qu'il est précisé dans la Norme sur l'accessibilité des sites Web : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601.

(v) **Inclusions.** L'entrepreneur déclare et certifie que les services comprennent ce qui suit :

i. l'hébergement et la tenue à jour de la solution, s'il y a lieu ;

ii. la fourniture de tous les services d'infrastructure de la technologie de l'information accessoires et supplémentaires requis, conformément à toutes les normes de sécurité requises;

iii. l'infrastructure technique qui respecte toutes les normes de sécurité requises, permettant au Canada d'utiliser la solution pour traiter les données de clients conformément à ses normes de sécurité exprimées, en plus d'un accès et d'une utilisation absolues par le client, indépendamment de la quantité de données créées, traitées ou stockées par la solution,

tous ces éléments étant inclus dans le prix.

(vi) **Droits d'utilisation restreints.** Le Canada reconnaît qu'en fournissant les services, l'entrepreneur ne cède pas de droits de propriété d'un produit logiciel, d'une composante de la solution ou de l'infrastructure utilisée par l'entrepreneur pour fournir les services, sauf ce qui est prévu expressément dans une autorisation de tâche. Le Canada ne fera sciemment pas les choses suivantes :

i. distribuer, octroyer une licence, prêter ou vendre la solution;

ii. affaiblir ou contourner les mécanismes de sécurité de la solution;

iii. retirer, modifier ou obscurcir tout avis de droit d'auteur, de marque commerciale ou tout autre avis de propriété figurant sur ou dans la solution.

(vii) **Conditions applicables**. L'entrepreneur a indiqué, et le Canada a reconnu, que l'entrepreneur peut modifier unilatéralement les modalités selon lesquelles il fournit son offre commerciale de la solution, sans préavis à ses clients, dont le Canada. L'entrepreneur déclare et certifie que de telles modifications n'entraîneront pas des conditions moins favorables, plus précisément en ce qui concerne le prix, le niveau de service et les recours, sans égard à tout avis contraire.

(viii) **Modalités supplémentaires**. Les parties conviennent que toute modalité, y compris les « cliquer et suivre » ou les avis « contextuels » qui s'appliquent à l'offre commerciale d'entrepreneur pour la solution, y compris les outils de tiers ou l'infrastructure connexe, ne s'appliquera pas à l'utilisation de la solution par le Canada si ces modalités entrent en conflit avec les conditions explicites de ce contrat. Les modalités des outils de tiers qui ne sont pas précisées dans le contrat ne sont pas assujetties à cette section.

7.8 Documentation

a) **Documentation de la solution.** L'entrepreneur doit fournir la documentation de la solution disponible sur le marché, ou y donner accès, au Canada à la suite de l'attribution du contrat. L'entrepreneur doit mettre à jour la documentation de la solution sur une base commercialement raisonnable.

b) **Autres documents.** L'entrepreneur doit fournir toute documentation, ou y donner accès, qui est nécessaire à l'exécution des travaux.

c) **Droits de traduction.** L'entrepreneur accepte que le Canada peut traduire tout livrable écrit, y compris la documentation de la solution et le matériel de formation, vers l'anglais ou le français. L'entrepreneur reconnaît que le Canada est propriétaire de la traduction et qu'il n'a aucune obligation de fournir une traduction à l'entrepreneur. Tous les documents qui sont traduits par le Canada doivent inclure l'avis de droit d'auteur et de droit de propriété qui faisait partie du document original. L'entrepreneur ne sera pas tenu responsable des erreurs techniques qui se produisent en raison d'une traduction faite par le Canada.

d) **Droits moraux.** À la demande du Canada, l'entrepreneur peut fournir une renonciation écrite permanente aux droits moraux, dans une forme acceptable pour le Canada, de la part de tous les auteurs qui ont contribué au livrable écrit. Si l'entrepreneur est ne peut pas ou ne veut pas obtenir les renonciations demandées, il accepte de rendre le Canada indemne de toute perte et de toute dépense (y compris les frais juridiques) découlant d'une demande concernant la violation aux droits moraux présentée par un tiers d'après la traduction de la documentation écrite par le Canada.

e) **Documentation défectueuse.** Si, à tout moment de la durée du contrat, le Canada avise l'entrepreneur d'un défaut ou d'une non-conformité dans une partie de la documentation livrée avec les travaux, l'entrepreneur corrigera le défaut ou la non-conformité dès que possible, et à ses propres frais. Le Canada peut fournir à l'entrepreneur des renseignements sur des défauts ou des aspects non conformes dans d'autres documents, y compris la documentation de la solution, à titre d'information seulement.

7.9 Services professionnels facultatifs, services de formation optionnels, services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant).

a) **Services professionnels.** L'entrepreneur doit exécuter et livrer de tels services professionnels (les « travaux ») au Canada au fur et à mesure des besoins, de la façon exposée en détail dans une autorisation de tâche.

b) **Services de formation.** L'entrepreneur doit exécuter et livrer de tels services de formation (les « travaux ») au Canada au fur et à mesure des besoins, de la façon exposée en détail dans une autorisation de tâche.

c) **Services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant).** L'entrepreneur doit exécuter et fournir ces services de soutien (les « travaux ») au Canada au fur et à mesure des besoins, tel qu'indiqué dans une autorisation de tâches.

d) **Déroulement des travaux; garantie.** L'entrepreneur déclare et atteste ce qui suit : a) il dispose de tout ce qui est nécessaire pour exécuter les travaux; b) il possède tout ce qu'il faut pour exécuter les travaux, y compris les ressources, les installations, la main-d'œuvre, la technologie, l'équipement et les matériaux; b) il a les qualifications nécessaires, incluant les connaissances, le savoir-faire et l'expérience, et la capacité de les utiliser efficacement pour exécuter les travaux.

e) **Rigueur des délais.** Il est essentiel que les travaux soient livrés dans les délais prévus dans une autorisation de tâche.

f) **Personnel autorisé.** Tous les travaux doivent être effectués par du personnel autorisé uniquement de l'entrepreneur.

g) **Personnel clé.** Lorsque le contrat précise l'identité des personnes qui doivent exécuter les travaux, l'entrepreneur est tenu de fournir les services de ces personnes. Si l'entrepreneur ne peut pas fournir les services d'une personne désignée dans le contrat, il doit fournir les services d'un remplaçant qui possède des qualifications et une expérience équivalentes et donner au Canada un préavis écrit indiquant (i) la raison du remplacement, (ii) le nom et les qualifications du remplaçant et (iii) la preuve que le remplaçant possède l'attestation de sécurité exigée.

h) **Demande de remplacement de personnel clé.** L'autorité contractante peut demander qu'un remplaçant cesse l'exécution des travaux. L'entrepreneur doit alors se conformer sans délai à cet ordre et retenir les services d'un autre remplaçant conformément aux conditions de remplacement du personnel clé. Le fait que l'autorité contractante n'ordonne pas qu'un remplaçant cesse d'accomplir les travaux ne libère pas l'entrepreneur de son obligation de répondre aux exigences du contrat.

i) **Migration.** L'entrepreneur reconnaît qu'en raison de la nature des services fournis en vertu du contrat, le Canada peut exiger la continuité. Avant la transition vers le nouvel entrepreneur ou au Canada, l'entrepreneur devra fournir toute l'information et la documentation opérationnelle, technique, conceptuelle et les renseignements pour la configuration nécessaires à la transition de tous les services, dans la mesure où il ne s'agit pas de renseignements confidentiels de l'entrepreneur. L'entrepreneur déclare et certifie qu'il ne s'ingérera pas directement ou indirectement dans l'accès du Canada aux données du client ou leur transfert, ou qu'il n'y nuira pas directement ou indirectement.

j) **Services de migration et de transition.** L'entrepreneur convient que, durant la période menant à la fin du contrat, si des services de migration ou de transition sont demandés par le Canada, il aidera diligemment le Canada pendant la transition entre ce contrat et le nouveau contrat conclu avec le nouvel entrepreneur, ou pendant la migration des données du client

vers un nouvel environnement de fournisseur. De plus, les services ci-dessous ainsi assurés ne donneront lieu à aucun autre frais que ceux qui sont prévus dans la base de paiement.

7.10 Réparations

a) **Travaux.** Si à tout moment pendant la durée du contrat, les travaux ne respectent pas leurs obligations de garantie, l'entrepreneur doit le plus tôt possible, à la demande du Canada, corriger à ses propres frais toute erreur ou tout défaut et apporter les modifications nécessaires aux travaux.

b) **Documentation.** Si à tout moment pendant la période du contrat, le Canada découvre un défaut ou une non-conformité dans une partie de la documentation livrée avec les travaux, l'entrepreneur doit corriger le plus tôt possible à ses propres frais le défaut ou la non-conformité.

c) **Droit du Canada à une réparation.** Si l'entrepreneur ne s'acquitte pas d'une obligation prévue aux présentes dans un délai raisonnable après avoir reçu un avis, le Canada aura le droit de remédier ou de faire remédier aux travaux défectueux ou non conformes aux frais de l'entrepreneur. Si le Canada ne désire pas corriger ou remplacer les travaux défectueux ou non conformes, le prix contractuel sera réduit de façon équitable.

7.11 Contrats de sous-traitance

a) **Conditions de sous-traitance.** L'entrepreneur peut sous-traiter l'exécution des travaux, pourvu que a) l'entrepreneur obtienne le consentement écrit préalable du Canada, b) le sous-traitant est lié par les termes du présent contrat, et c) l'entrepreneur demeure responsable envers le Canada pour tous les travaux effectués par le sous-traitant.

b) **Exceptions au consentement à la sous-traitance.** L'entrepreneur n'est pas tenu d'obtenir le consentement de l'autorité contractante à l'égard des contrats de sous-traitance expressément autorisés dans le contrat. L'entrepreneur peut également, sans le consentement de l'autorité contractante : (i) acheter des produits courants en vente libre dans le commerce, ainsi que des articles et des matériaux produits par des fabricants dans le cours normal de leurs affaires; (ii) sous-traiter des services accessoires qui seraient ordinairement donnés en sous-traitance pendant l'exécution des travaux; et (iii) permettre à ses sous-traitants à tout échelon d'effectuer des achats ou de sous-traiter comme le prévoient les alinéas (i) et (ii).

7.12 Retard justifiable

a) Aucune responsabilité. L'entrepreneur n'est pas responsable des retards d'exécution ni de l'inexécution dus à des causes indépendantes de sa volonté qui ne pouvaient raisonnablement être prévues ou évitées par des moyens raisonnablement accessibles à l'entrepreneur, pourvu que l'entrepreneur informe l'autorité contractante de l'existence du retard ou de la probabilité du retard dès qu'il en est informé (appelé « retard justifiable »).

b) Avis. L'entrepreneur doit de plus informer l'autorité contractante, dans les 15 jours ouvrables, de toutes les circonstances liées au retard et soumettre à l'approbation de l'autorité contractante un plan de redressement clair qui détaille les étapes que l'entrepreneur propose de suivre afin de minimiser les conséquences de l'événement qui a causé le retard.

c) Dates de livraison et d'échéance : Toute date de livraison ou autre date qui est directement touchée par un retard justifiable fera l'objet d'un report raisonnable dont la durée n'excédera pas la durée du retard justifiable.

d) Le Canada n'est pas responsable des coûts : Le Canada ne sera pas responsable des frais engagés par l'entrepreneur ou l'un de ses sous-traitants ou mandataires par suite d'un retard

justifiable, sauf lorsque celui-ci est attribuable à l'omission du Canada de s'acquitter d'une de ses obligations en vertu du contrat.

7.13 Droit de résiliation

a) Si un tel événement empêche l'exécution du contrat pendant plus de 30 jours civils, l'autorité contractante peut alors choisir de résilier l'AT ou une partie ou la totalité du présent contrat sans qu'il y ait faute, ce qui signifie qu'aucune des parties ne sera responsable envers l'autre relativement au retard justifiable ou à la résiliation subséquente, et le Canada ne sera responsable que du paiement des services reçus à la date effective de la résiliation.

7.14 Inspection et acceptation des travaux

a) Inspection par le Canada : Tous les travaux sont soumis à l'inspection et à l'acceptation par le Canada. L'inspection et l'acceptation des travaux par le Canada ne relèvent pas l'entrepreneur de sa responsabilité à l'égard des défectuosités ou des autres manquements aux exigences du contrat. Le Canada est en droit de rejeter les travaux qui ne sont pas réalisés en conformité avec les exigences du contrat, et l'entrepreneur doit corriger ou remplacer les travaux à ses propres frais.

b) Procédures d'acceptation : Sauf disposition contraire du contrat, les procédures d'acceptation sont les suivantes :

   a. Une fois les travaux terminés, l'entrepreneur doit aviser par écrit l'autorité technique, avec copie à l'autorité contractante, en se référant à cette disposition du contrat et en demandant l'acceptation des travaux;

   b. Le Canada disposera de 30 jours à compter de la réception de l'avis pour effectuer son inspection (la « période d'acceptation »).

c) Défauts et soumission à nouveau des produits livrables : Si le Canada donne avis de l'existence d'une lacune pendant la période de réception, l'entrepreneur doit corriger la lacune le plus tôt possible et aviser le Canada par écrit une fois les travaux terminés, après quoi le Canada aura le droit de procéder à une nouvelle inspection des travaux avant la réception et la période de réception recommencera. Si le Canada détermine qu'un produit livrable est incomplet ou déficient, il n'est pas tenu de désigner tous les articles manquants ou tous les défauts avant de rejeter le produit livrable.

d) Accès aux lieux : L'entrepreneur doit permettre aux représentants du Canada, en tout temps durant les heures de travail, d'accéder à tous les lieux où toute partie des travaux est exécutée, outre les centres de données à multiples locataires. Les représentants du Canada peuvent procéder à leur gré à des examens et à des vérifications. L'entrepreneur doit fournir toute l'aide, les locaux, tous les échantillons, pièces d'essai et documents que les représentants du Canada peuvent raisonnablement exiger pour l'exécution de l'inspection. L'entrepreneur doit expédier lesdits échantillons et pièces d'essai à la personne ou à l'endroit indiqué par le Canada.

e) Inspection de la qualité par l'entrepreneur : L'entrepreneur doit inspecter et approuver toute partie des travaux avant de le soumettre pour acceptation ou livraison au Canada. Tous les produits livrables soumis par l'entrepreneur doivent être d'une qualité professionnelle, exempts d'erreurs typographiques et autres erreurs, et conformes aux normes les plus élevées de l'industrie.

f) Registre des inspections : L'entrepreneur doit tenir un registre des inspections à la fois précis et complet qu'il doit mettre à la disposition du Canada, sur demande. Les représentants du Canada peuvent tirer des copies et des extraits des registres pendant l'exécution du contrat et pendant une période maximale de trois ans après la fin du contrat.

g) Rétroaction informelle : À la demande de l'entrepreneur, le Canada peut fournir une rétroaction informelle avant que tout produit livrable ne soit officiellement soumis pour acceptation.

Toutefois, cela ne doit pas être utilisé comme une forme de contrôle de la qualité des travaux de l'entrepreneur. Le Canada n'est pas tenu de fournir une rétroaction informelle.

7.15 Réunion de lancement

a) L'entrepreneur doit planifier une réunion de lancement en présence du client et de l'autorité contractante de SPAC afin de discuter du besoin en général, de l'approche et de la méthode, du contrat, de l'établissement des projets, de la gestion de l'échéancier et de toute question à éclaircir. La réunion doit avoir lieu avant de commencer des travaux et à un endroit accepté mutuellement, ou par téléconférence. Le président de la réunion sera l'autorité contractante.

b) L'entrepreneur doit préparer et distribuer l'ordre du jour de la réunion et le soumettre dans un délai raisonnable à l'autorité contractante aux fins d'approbation, avant sa distribution à toutes les autorités.

c) L'entrepreneur doit fournir l'ordre du jour et une présentation, moins de 2 jours ouvrables avant la date de début de la réunion.

d) L'entrepreneur doit préparer le procès-verbal de la réunion et le fournir dans un délai de 2 jours ouvrables à l'autorité contractante aux fins d'approbation, avant sa distribution à toutes les autorités.

7.16 Réunion d'examen des progrès

a) L'autorité contractante et l'entrepreneur peuvent, à tout moment, convoquer une réunion pour discuter des travaux et d'examiner leurs progrès par rapport au présent contrat. Une telle réunion doit avoir lieu après avoir donné préavis à l'autre partie, et elle doit normalement être organisée par téléconférence. Le président de la réunion sera l'autorité contractante ou la partie demandant la réunion.

b) L'entrepreneur doit préparer l'ordre du jour de la réunion et le distribuer à toutes les autorités.

c) L'entrepreneur doit préparer l'ordre du jour de la réunion et le soumettre dans un délai raisonnable à l'autorité contractante aux fins d'approbation, avant sa distribution à toutes les autorités.

d) L'entrepreneur devra fournir la présentation et les points à l'ordre du jour achevés cinq (5) jours ouvrables avant la date de début de la réunion.

e) L'entrepreneur doit préparer le procès-verbal de la réunion et le soumettre dans un délai de 15 jours ouvrables à l'autorité contractante aux fins d'approbation, avant sa distribution à toutes les autorités.

7.17 Autorisation de tâche

a) La prestation par l'entrepreneur de services professionnels, de services de formation, de Services de maintenance et de soutien de la solution (le cas échéant) ou services d'hébergement et de soutien liés à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant) en vertu du présent contrat sera effectuée « au fur et à mesure des besoins » au moyen d'une autorisation de tâches (AT).

b) Forme et contenu de l'AT. Une AT contiendra (a) le contrat et le numéro de tâche, (b) les détails concernant les biens et les services et les activités à exécuter et les ressources requises, (c) une description des produits livrables, (d) un calendrier indiquant les dates d'achèvement des activités principales et les dates de présentation des produits livrables, (e) les exigences relatives à la sécurité, et (f) les coûts. Une AT suivra le format exposé en détail à l'annexe F – Formulaires d'autorisation de tâche.

c) Réponse de l'entrepreneur à une AT. L'entrepreneur doit fournir au Canada, dans la période mentionnée dans l'autorisation de tâche, le coût estimatif total proposé pour l'exécution du travail et une répartition des coûts, établie conformément aux honoraires. L'entrepreneur ne sera pas payé pour la préparation ni la présentation d'une réponse ou pour la communication d'autres renseignements requis pour la préparation et l'attribution de l'autorisation de tâche approuvée.

d) Limite des autorisations de tâches et pouvoirs relatifs à l'attribution officielle d'AT. Pour être attribuée de façon officielle, une autorisation de tâche doit être signée par l'autorité canadienne concernée comme indiqué dans le présent contrat. Tous les travaux entrepris par l'entrepreneur sans que celui-ci ait reçu une autorisation de tâche valide seront effectués à ses propres risques.

e) **Rapports d'utilisation périodiques.** L'entrepreneur doit compiler et tenir à jour des données sur les services fournis au gouvernement fédéral conformément aux AT approuvées émises dans le cadre du contrat.

f) **Regroupement d'autorisations de tâches pour des raisons administratives.** Le contrat peut être modifié à l'occasion afin de tenir compte de l'ensemble des autorisations de tâches valides émises à ce jour et de consigner les travaux réalisés dans le cadre de ces autorisations de tâches à des fins administratives.

7.18 Exigences relatives à la sécurité

Le Canada se réserve le droit de mettre à jour les exigences relatives à la sécurité.

a) **Fournisseur canadien**

(i) Le contractant ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ B, délivrées par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

(ii) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une COTE DE FIABILITÉ valide, délivrée ou approuvée par la DSIC/SPAC.

(iii) L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements PROTÉGÉS tant que la DSIC de TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée ou approuvée, ces tâches pourront être exécutées au niveau PROTÉGÉ B (y compris un lien électronique au niveau PROTÉGÉ B).

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

(v) L'entrepreneur ou l'offrant devra respecter les dispositions:

i. de la liste de vérification des exigences en matière de sécurité et la directive de sécurité (s'il y a lieu), ci-jointes à l'annexe C;

ii. du Manuel de la sécurité industrielle (plus récente édition).

b) **Fournisseur étranger**

L'administration désignée en matière de sécurité (ADS canadienne) pour les questions industrielles au Canada est le Secteur de la sécurité industrielle (SSI), Travaux publics et Services gouvernementaux Canada (TPSGC), administré par la Direction de la sécurité

industrielle internationale (DSII). L'ADS canadienne est chargée d'évaluer la conformité de l'**entrepreneur** ou du **sous-traitant** aux exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux **entrepreneurs et aux sous-traitants** étrangers destinataires qui sont constitués en personne morale ou autorisés à faire des affaires dans un État autre que le Canada et à livrer ou exécuter la solution, en plus des exigences relatives à la vie privée et à la sécurité. Ces exigences en matière de sécurité s'ajoutent aux exigences déjà déterminées ci-dessous dans la section Protection et sécurité des données emmagasinées dans des bases de données.

(i) L'**entrepreneur ou le sous-traitant** étranger destinataire doit provenir d'un pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Union européenne (UE) ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité industrielle. Le Programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatérale ou multinationale industrielle avec les pays mentionnés au site suivant de TPSGC : https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

(ii) L'**entrepreneur ou le sous-traitant** étranger destinataire doit en tout temps, au cours de la durée du **contrat ou du contrat de sous-traitance**, être inscrit auprès de l'autorité nationale de supervision de la protection des renseignements personnels appropriée des pays dans lesquels il est incorporé, autorisé à exercer des activités commerciales ou en opération. L'entrepreneur ou le sous-traitant étranger destinataire doit fournir à l'autorité contractante et au chargé de projet une preuve de leur inscription auprès de l'ADS canadienne et de l'autorité nationale de supervision de la protection des renseignements personnels appropriée, ainsi que le nom de cette dernière. Pour les **entrepreneurs et les sous-traitants** européens, l'autorité nationale sera l'autorité de protection des données.

(iii) L'**entrepreneur ou le sous-traitant** étranger destinataire doit détenir en permanence, pendant l'exécution du contrat, une équivalence d'une attestation de vérification d'organisation désignée en vigueur, délivrée par l'ADS canadienne, comme suit :

i. L'**entrepreneur ou le sous-traitant** étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence.

ii. L'**entrepreneur ou le sous-traitant** étranger destinataire ne doit pas entreprendre les travaux, fournir les services ou assurer toute autre prestation tant que l'administration désignée en matière de sécurité canadienne (ADS canadienne) n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le contrat. L'ADS canadienne fournira, par écrit, à l'**entrepreneur ou au sous-traitant** étranger destinataire un formulaire d'attestation qui confirmera la conformité et l'autorisation de fournir les services prévus.

iii. L'**entrepreneur ou le sous-traitant** étranger destinataire doit identifier un agent de sécurité des contrats (ASC) autorisé et un agent remplaçant de sécurité des contrats (ARSC) qui sera responsable du contrôle des exigences de sécurité, telles qu'elles sont définies dans le présent **contrat ou contrat de sous-traitance**. Cette personne sera nommée par le président-directeur général de l'**entrepreneur ou du sous-traitant** étranger destinataire qui présente une soumission ou par un cadre supérieur principal désigné, qui est soit propriétaire, dirigeant, agent, administrateur, directeur ou partenaire, et qui occupe un poste qui lui permettrait d'influer de manière négative sur les politiques ou les pratiques de l'organisation dans l'exécution du **contrat ou du contrat de sous-traitance**.

iv. L'**entrepreneur ou le sous-traitant** étranger destinataire donne accès à des **renseignements personnels** et biens de niveau **PROTÉGÉ B AU CANADA** seulement à son personnel, aux conditions suivantes :

1) le personnel a un besoin de savoir pour l'exécution du **contrat ou du contrat de sous-traitance**;

2) b. le casier judiciaire et les antécédents des membres du personnel ont fait l'objet d'une vérification par un organisme gouvernemental ou du secteur privé reconnu de **leur pays** ainsi que d'une vérification des antécédents validée par l'ADS canadienne;

3) l'**entrepreneur ou le sous-traitant** étranger destinataire doit veiller à ce que ses employés consentent à ce que les résultats de la vérification de leur casier judiciaire et de leurs antécédents soient communiqués à l'ADS canadienne et à d'autres fonctionnaires du gouvernement canadien, au besoin;

4) le gouvernement du Canada se réserve le droit de refuser l'accès à des renseignements ou biens de niveau **PROTÉGÉ AU CANADA** à un **entrepreneur ou sous-traitant** étranger destinataire pour un motif valable.

(iv) Les **renseignements personnels** et les biens **DE NIVEAU PROTÉGÉ DU CANADA** qui sont fournis à l'**entrepreneur ou au sous-traitant** étranger destinataire, ou qui sont produits par ce dernier, doivent respecter les conditions suivantes :

i. Ils ne doivent pas être divulgués à un autre gouvernement, personne ou entreprise qui n'est pas directement lié à l'exécution du **contrat ou du contrat de sous-traitance** sans le consentement écrit préalable du Canada. Ce consentement doit être obtenu auprès de son autorité de protection des données (APD) et de l'autorité contractante (en collaboration avec l'ASD canadienne).

ii. Ils ne doivent pas être utilisés à des fins autres que l'exécution du **contrat ou du contrat de sous-traitance**, sans l'approbation écrite préalable du Canada. Cette approbation doit être obtenue auprès de son autorité de protection des données (APD) et l'autorité contractante (en collaboration avec la ASD canadienne).

(v) Tant que l'administration **l'entrepreneur / le sous-traitant** étranger destinataire n'a pas transmis à l'ADS canadien les attestations de sécurité écrites exigées pour les membres du personnel de **l'entrepreneur / du sous-traitant** étranger destinataire, ces derniers **NE PEUVENT PAS AVOIR ACCÈS** aux renseignements/biens de niveau **CANADA PROTÉGÉ A ou B et NE PEUVENT PAS PÉNÉTRER** sur les sites du « gouvernement du Canada » ou de l'« entrepreneur » où ces renseignements et ces biens sont conservés à moins d'être accompagnés. L'escorte de sécurité doit être un employé du « gouvernement du Canada » ou de l'« entrepreneur » détenant une Attestation de sécurité du personnel au niveau exigé.

(vi) L'**entrepreneur ou le sous-traitant** étranger destinataire doit en tout temps, au cours de la durée du **contrat ou du contrat de sous-traitance**, doit détenir l'équivalent d'une autorisation de détenir des renseignements (ADR) au niveau **PROTÉGÉ B AU CANADA**. Tous les **renseignements personnels** et les biens de niveau **PROTÉGÉ AU CANADA** fournis à l'**entrepreneur ou au sous-traitant** étranger destinataire ou produits par l'étranger destinataire (**entrepreneur et sous-traitant**) doivent également être protégés comme suit :

(vii) L'**entrepreneur ou le sous-traitant** étranger destinataire reconnaît et convient que toutes ses obligations en matière de protection et de gestion des renseignements personnels en vertu du **contrat ou du contrat de sous-traitance** s'ajoutent à toutes leurs obligations en vertu de la législation nationale sur la vie privée des pays dans lesquels il est incorporé ou en opération.

(viii) **L'entrepreneur ou le sous-traitant** étranger destinataire NE DOIT PAS emporter de renseignements/ biens de niveau **CANADA PROTÉGÉ** hors des établissements de travail visés, et **l'entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

(ix) L'**entrepreneur ou le sous-traitant** étranger destinataire ne devra pas utiliser les **renseignements personnels** ni les biens de **niveau PROTÉGÉ AU CANADA** pour répondre à des besoins autres que l'exécution du **contrat** sans l'approbation écrite préalable du gouvernement du Canada. Cette approbation doit être obtenue auprès de l'ADS canadienne.

(x) L'**entrepreneur ou le sous-traitant** étranger destinataire devra signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait ou a lieu de croire que des **renseignements personnels** ou des biens de **niveau PROTÉGÉ AU CANADA** relatifs à l'exécution du présent **contrat** ont été compromis.

(xi) L'**entrepreneur ou le sous-traitant** étranger destinataire devra signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait ou a lieu de croire que des **renseignements personnels** ou des biens de **niveau PROTÉGÉ AU CANADA** auxquels l'**entrepreneur ou le sous-traitant** a eu accès dans l'exécution du **contrat** ont été perdus ou remis à des personnes non autorisées.

(xii) L'**entrepreneur ou le sous-traitant** étranger destinataire ne doit pas divulguer les **renseignements personnels de niveau PROTÉGÉ AU CANADA** à un autre gouvernement, ni à une autre personne physique ou morale, ni non plus à leurs représentants, sans l'accord écrit préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS canadienne.

(xiii) L'**entrepreneur ou le sous-traitant** étranger destinataire doit assurer une protection des **renseignements personnels** et des biens de **niveau PROTÉGÉ AU CANADA** aussi stricte que celle assurée par le gouvernement du Canada, conformément aux politiques nationales ainsi qu'aux lois et règlements en matière de sécurité nationale, et dans le respect des prescriptions prévues par l'ADS canadienne.

(xiv) À la fin des travaux, l'**entrepreneur ou le sous-traitant** étranger destinataire doit remettre au gouvernement du Canada tous les **renseignements personnels** et biens **de niveau PROTÉGÉ AU CANADA** fournis ou produits en vertu du contrat ou du contrat de sous-traitance, y compris tous les renseignements et biens de niveau PROTÉGÉ AU CANADA remis à ses sous-traitants ou produits par eux.

(xv) L'**entrepreneur ou le sous-traitant** étranger destinataire qui doit accéder à des **renseignements personnels** ou à des biens de niveau **PROTÉGÉ DU CANADA** ou à des sites à accès restreint au Canada en vertu du présent **contrat** doit soumettre une demande d'accès au site à l'agent de sécurité ministériel d'Environnement et Changement climatique Canada.

(xvi) L'**entrepreneur ou le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker dans un système informatique (et transférer au moyen d'un lien électronique) des **renseignements personnels** et des biens de **niveau PROTÉGÉ B AU CANADA** avant que l'ADS canadienne lui en donne le droit.

(xvii) L'**entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que les clauses de sécurité appropriées, conformément aux exigences de l'ASD canadienne, sont ajoutées aux contrats de sous-traitance donnant accès à des **renseignements personnels** ou à des biens de niveau PROTÉGÉ DU CANADA fournis ou générés dans le cadre du présent **contrat ou contrat de sous-traitance**. Il doit également s'assurer que toutes les conditions sont non moins favorables au Canada que les conditions établies dans les exigences en matière de sécurité.

(xviii) Si un **entrepreneur ou un sous-traitant** étranger destinataire est choisi comme fournisseur dans le cadre du présent **contrat ou contrat de sous-traitance**, des clauses de sécurité propres au pays doivent être établies et publiées par l'ADS canadienne; ces clauses seront fournies à l'autorité contractante du gouvernement du Canada, afin de respecter les dispositions de sécurité relatives aux équivalences établies par l'ADS canadienne.

(xix) Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne.

(xx) L'**entrepreneur ou le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'annexe « C ».

(xxi) Le Canada a le droit de rejeter toute demande visant l'accès électronique aux **renseignements personnels** et biens de **niveau PROTÉGÉ AU CANADA** liés aux travaux dans un autre pays ainsi que le traitement, la production, la transmission ou l'entreposage de ces renseignements s'il y a des raisons de croire que leur sécurité, leur confidentialité ou leur intégrité pourrait être menacée.

c) **Protection et sécurité des données stockées dans des bases de données**

(i) L'**entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que toutes les bases de données utilisées par des organisations pour fournir les services décrits dans la solution proposée **qui contiennent des renseignements personnels de** niveau PROTÉGÉ AU CANADA relativement aux travaux se trouvent au Canada.

(ii) L'**entrepreneur ou le sous-traitant** étranger destinataire doit contrôler l'accès à toutes les bases de données dans lesquelles sont stockées des données liées au présent **contrat ou le contrat de sous-traitance**, afin que seules les personnes titulaires de la cote de sécurité appropriée puissent avoir accès à la base de données, soit au moyen d'un mot de passe ou d'un autre moyen d'accès (comme des mesures de contrôle biométrique).

(iii) L'**entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que toutes les bases de données comprenant des données relatives au présent **contrat ou contrat de sous-traitance** et archivées sont isolées sur les plans physique et logique, en d'autres termes qu'elles n'ont aucune connexion directe ou indirecte de quelque type que ce soit avec d'autres bases de données.

(iv) L'**entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que toutes les données liées au **contrat ou au contrat de sous-traitance** sont traitées uniquement au Canada ou dans un autre pays approuvé par l'autorité contractante conformément au paragraphe de la sous-section b) (i).

(v) L'**entrepreneur ou le sous-traitant** étranger destinataire doit s'assurer que le trafic sur le réseau national (c'est-à-dire le trafic partant d'une partie du Canada vers une destination située dans une autre partie du Canada) s'effectue exclusivement au Canada, sauf si l'autorité contractante a approuvé au préalable, par écrit, une autre route. L'autorité contractante prendra uniquement en considération une route dans un autre pays pour la transmission des données, si ce pays respecte les exigences décrites au paragraphe de la sous-section b) (i).

(vi) Malgré tout article des conditions générales relatif à la sous-traitance, l'**entrepreneur ou le sous-traitant** étranger destinataire ne peut confier à un sous-traitant (y compris à une société affiliée) aucune fonction qui permet d'accéder aux données du contrat sans le consentement écrit préalable de l'autorité contractante (en collaboration avec l'ADS canadienne).

d) **Renseignements personnels**

(i) **Interprétation**

i. Dans le présent **contrat ou contrat de sous-traitance**, les définitions suivantes s'appliquent, sauf indication contraire :

« conditions générales » désignent les conditions générales qui font partie du **contrat ou du contrat de sous-traitance**;

« renseignement personnel » désigne tout renseignement qui concerne un individu, y compris le type de renseignements décrit dans la *Loi sur la protection des renseignements personnels, L.R.C. 1985*, ch. P-21;

« dossier » désigne un exemplaire papier ou des données sous forme lisible par machine comprenant des renseignements personnels.

ii. Les mots et expressions définis dans les conditions générales et utilisés dans les présentes conditions générales supplémentaires ont le sens qui leur est donné dans les conditions générales.

iii. Dans l'éventualité d'incompatibilité entre les conditions générales et ces conditions générales supplémentaires, les dispositions pertinentes des ces conditions générales supplémentaires prévalent.

e) **Propriété des renseignements personnels et des dossiers**

Pour exécuter les travaux, l'**entrepreneur ou le sous-traitant** étranger destinataire aura accès à des renseignements personnels de tiers et(ou) en recueillera. L'**entrepreneur ou le sous-traitant** reconnaît qu'il n'a aucun droit sur ces renseignements personnels ou dossiers et que ces derniers appartiennent au Canada. L'**entrepreneur ou le sous-traitant** étranger destinataire doit immédiatement, sur demande, mettre tous les renseignements personnels et tous les dossiers à la disposition du Canada dans un format acceptable pour le Canada.

f) **Utilisation des renseignements personnels**

L'**entrepreneur ou le sous-traitant** étranger destinataire convient de créer, recueillir, recevoir, gérer, utiliser et conserver des renseignements personnels et des dossiers de même que d'y avoir accès et d'en disposer uniquement pour exécuter les travaux conformément au **contrat ou au contrat de sous-traitance**.

g) **Collecte de renseignements personnels**

(i) Si **l'entrepreneur/le sous-traitant** étranger destinataire doit obtenir des renseignements personnels d'un tiers dans le cadre des travaux, il ne doit recueillir que les renseignements personnels lui permettant d'exécuter les travaux. **L'entrepreneur/Le sous-traitant** étranger destinataire doit recueillir les renseignements personnels auprès de l'individu concerné et l'informer (au moment de la cueillette ou préalablement) de ce qui suit :

i. les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;

ii. les usages qui seront faits des renseignements personnels recueillis;

iii. que la divulgation des renseignements personnels est volontaire ou, s'il existe une obligation juridique de divulguer les renseignements personnels, les fondements de cette obligation juridique;

iv. les conséquences, le cas échéant, du refus de fournir les renseignements;

v. que l'intéressé a le droit d'accéder à ses renseignements personnels et d'y apporter des corrections;

vi. que les renseignements personnels feront partie d'un fichier de renseignements personnels particulier (au sens de la *Loi sur la protection des renseignements personnels*), et fournir à l'individu de l'information concernant l'institution fédérale qui gère le fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements à l'**entrepreneur/au sous-traitant** étranger destinataire.

(ii) L'entrepreneur étranger destinataire, ses sous-traitants et leurs employés respectifs doivent s'identifier auprès des individus desquels ils recueillent des renseignements personnels et leur donner le moyen de vérifier qu'ils sont autorisés à recueillir les renseignements personnels en vertu d'un contrat passé avec le Canada.

(iii) Si l'autorité contractante l'exige, l'**entrepreneur /le sous-traitant** étranger destinataire doit élaborer un formulaire de demande de consentement à utiliser lors de la cueillette de renseignements personnels ou un texte dans le cas de la cueillette de renseignements personnels par téléphone. L'**entrepreneur/Le sous-traitant** étranger destinataire ne peut utiliser le formulaire ou le texte sans avoir obtenu l'approbation écrite préalable de l'autorité contractante. Il doit aussi obtenir le consentement de l´autorité contractante avant de modifier le formulaire ou le texte.

(iv) Si, lors de la cueillette de renseignements personnels auprès d'un individu, l'**entrepreneur/le sous-traitant** étranger destinataire sait ou soupçonne que cet individu n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, l'**entrepreneur/le sous-traitant** étranger destinataire doit demander des directives à l'administration désignée en matière de sécurité pour le contrat.

h) **Exactitude, confidentialité et intégrité des renseignements personnels**

L'**entrepreneur ou le sous-traitant** étranger destinataire doit veiller à ce que les renseignements personnels soient les plus exacts, complets et à jour que possible. L'**entrepreneur ou le sous-traitant** étranger destinataire doit assurer la confidentialité des renseignements personnels. Pour ce faire, l'**entrepreneur/le sous-traitant** étranger destinataire doit, au minimum :

(i) ne pas utiliser de données d'identification personnelle (p. ex., le numéro d'assurance sociale) pour lier de nombreuses bases de données qui comprennent des renseignements personnels;

(ii) isoler tous les dossiers des renseignements et des dossiers de **l'entrepreneur/du sous-traitant** étranger destinataire;

(iii) ne donner l'accès aux renseignements personnels et aux dossiers qu'aux personnes qui en ont besoin aux fins d´exécution des travaux (par exemple, en utilisant des mots de passe ou un accès biométrique);

(iv) donner de la formation à toute personne à laquelle **l'entrepreneur/le sous-traitant** étranger destinataire donne accès aux renseignements personnels concernant l'obligation d'assurer la confidentialité et de ne l'utiliser qu'aux fins d'exécution des travaux. **L'entrepreneur/Le sous-traitant** étranger destinataire doit donner cette formation avant d'autoriser l'accès aux renseignements personnels et préparer à cet effet un dossier accessible à l'autorité contractante, sur demande;

(v) à la demande de l'autorité contractante, demander aux personnes ayant accès aux renseignements personnels de reconnaître, par écrit (sous une forme approuvée par l'autorité contractante), leurs responsabilités en matière de confidentialité des renseignements personnels, avant de leur en donner l'accès;

(vi) tenir un registre de toutes les demandes faites par un individu pour la révision de ses renseignements personnels et toutes les demandes de correction d'erreurs ou

d'omissions concernant les renseignements personnels (que les demandes soient faites directement par un individu ou par le Canada au nom d'un individu);

(vii) joindre une note à tout dossier qu'un individu a demandé de corriger, mais que **l'entrepreneur/le sous-traitant** étranger destinataire a décidé, pour quelque raison que ce soit, de ne pas corriger. Lorsque cela se produit, l'entrepreneur doit immédiatement informer l'autorité contractante de la correction demandée et des raisons de **l'entrepreneur/le sous-traitant** étranger destinataire de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, l'entrepreneur a l'obligation de le faire;

(viii) tenir un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;

(ix) maintenir un journal de vérification électronique qui enregistre tous les accès et les tentatives d'accès des dossiers électroniques. Le journal de vérification doit être dans un format qui peut être lu par **l'entrepreneur/le sous-traitant** étranger destinataire et le Canada en tout temps; et

(x) sécuriser et contrôler l'accès à tout exemplaire papier des dossiers.

i) **Protection des renseignements personnels**

L'**entrepreneur/Le sous-traitant** étranger destinataire doit protéger les renseignements personnels à tout moment en prenant toutes les mesures raisonnablement nécessaires pour les protéger et en protéger l'intégrité et la confidentialité. Pour ce faire, l'**entrepreneur/le sous-traitant** étranger destinataire doit, au minimum :

(i) stocker les renseignements personnels sous format électronique de manière à ce qu'un mot de passe (ou un autre mécanisme de contrôle, comme l'accès biométrique) soit requis pour accéder au système ou à la base de données où sont stockés les renseignements personnels;

(ii) s'assurer que les mots de passe ou autres moyens d'accès aux renseignements personnels ne sont fournis qu'aux individus qui le requièrent aux fins d'exécution des travaux;

(iii) ne pas confier à un tiers (y compris un affilié) le stockage des renseignements personnels sans l'autorisation préalable et écrite de l'ADS canadienne;

(iv) protéger toutes les bases de données ou tous les systèmes informatiques qui contiennent des renseignements personnels contre un accès externe par des méthodes couramment utilisées par des organismes publics et privés du Canada faisant preuve de prudence dans le but de protéger les renseignements très protégés et sensibles;

(v) faire une sauvegarde et une mise à jour de tous les dossiers au moins une fois par semaine;

(vi) instaurer toutes les mesures raisonnables de sécurité et de protection que le Canada demande de temps à autre;

(vii) aviser immédiatement l'ADS canadienne de toute infraction à la sécurité, par exemple, chaque fois qu'un individu non autorisé obtient l'accès aux renseignements personnels.

j) **Nomination d'un agent de protection de la vie privée**

L'**entrepreneur ou le sous-traitant** étranger destinataire doit nommer quelqu'un comme agent de protection de la vie privée, qui agira en tant que son représentant pour toutes les questions touchant aux renseignements personnels et aux dossiers. L'**entrepreneur ou le sous-traitant** étranger destinataire doit indiquer le nom de cette personne à l'autorité contractante et à l'ADS canadienne dans les dix (10) jours suivant l'attribution du **contrat ou du contrat de sous-traitance**.

k) **Obligation de présenter des rapports trimestriels**

Dans un délai de trente (30) jours suivant la fin de chaque trimestre (janvier-mars; avril-juin; juillet-septembre; octobre-décembre), l'**entrepreneur ou le sous-traitant** étranger destinataire doit présenter ce qui suit à l'autorité contractante :

(i) une description de toute nouvelle mesure prise par l'**entrepreneur ou le sous-traitant** étranger destinataire afin de protéger les renseignements personnels (par exemple, l'utilisation par ce dernier de nouveaux logiciels ou contrôles d'accès);

(ii) une liste des corrections apportées aux renseignements personnels à la demande d'un individu concerné (comprenant le nom de la personne, la date de la demande et la correction apportée);

(iii) les détails de toute plainte reçue d'individus concernant la manière dont leurs renseignements personnels sont recueillis ou traités par l'**entrepreneur ou le sous-traitant**;

(iv) une copie (dans un format électronique convenu par l'autorité contractante et l'**entrepreneur ou le sous-traitant** étranger destinataire) de l'ensemble des renseignements personnels conservés électroniquement par l'**entrepreneur ou le sous-traitant**.

l) **Évaluation des menaces et des risques**

Dans les quatre-vingt-dix (90) jours civils suivant l'attribution du **marché** ou du **marché de sous-traitance**, et, si le **marché ou le marché de sous-traitance** dure plus d'un an, dans les trente (30) jours suivant chaque anniversaire du **marché** ou du **marché de sous-traitance**, l'**entrepreneur ou le sous-traitant** étranger destinataire doit présenter à l'autorité contractante et à l'ADS canadienne une évaluation des menaces et des risques, laquelle doit comprendre ce qui suit :

(i) une copie de la dernière version du formulaire de demande de consentement ou du texte que l'**entrepreneur ou le sous-traitant** étranger destinataire utilise pour recueillir les renseignements personnels;

(ii) une liste des types de renseignements personnels utilisés par l'**entrepreneur ou le sous-traitant** étranger destinataire relativement aux travaux;

(iii) la liste de tous les emplacements où les exemplaires papier des renseignements personnels sont conservés;

(iv) la liste de tous les endroits où les renseignements personnels lisibles par machine sont conservés (p. ex. l'emplacement des serveurs qui hébergent des bases de données contenant des renseignements personnels), y compris les copies de sauvegarde;

(v) une liste de toutes les personnes à qui l'**entrepreneur ou le sous-traitant** étranger destinataire a accordé un droit d'accès aux renseignements personnels ou aux documents;

(vi) une liste de toutes les mesures prises par l'**entrepreneur ou le sous-traitant** étranger destinataire pour protéger les renseignements personnels et les dossiers;

(vii) une explication détaillée des menaces réelles ou potentielles touchant les renseignements personnels ou les dossiers, accompagnée d'une évaluation des risques associés à ces menaces et la pertinence des mesures de protection contre ces risques en place;

(viii) une explication de toutes les nouvelles mesures de protection des renseignements personnels que l'**entrepreneur ou le sous-traitant** étranger destinataire prévoit mettre en œuvre pour protéger les renseignements personnels et les documents.

m) **Vérification**

Le Canada peut vérifier en tout temps la conformité de l'**entrepreneur/du sous-traitant** étranger destinataire avec ces conditions générales supplémentaires. À la demande de

l'autorité contractante, l'**entrepreneur/le sous-traitant** étranger destinataire doit donner au Canada (ou à son représentant autorisé) l'accès à ses locaux et aux renseignements personnels et dossiers en tout temps jugé raisonnable. Si le Canada découvre un problème durant la vérification, l'**entrepreneur/le sous-traitant** étranger destinataire doit le corriger immédiatement à ses frais.

n) **Obligations législatives**

(i) L'**entrepreneur/Le sous-traitant** étranger destinataire reconnaît que le Canada est tenu de traiter tous les renseignements personnels et les dossiers conformément aux dispositions de la *Loi sur la protection des renseignements personnels du Canada*, de la *Loi sur l'accès à l'information*, L.R.C. 1985, ch. A-1, et de la *Loi sur la Bibliothèque et les Archives du Canada*, L.C. 2004, ch.11. L'**entrepreneur/Le sous-traitant** étranger destinataire convient de se conformer aux exigences établies par l'autorité contractante qui sont requises pour permettre au Canada de remplir ses obligations en vertu de ces lois et toute autre loi qui entre en vigueur lorsqu'il y a lieu.

(ii) L'entrepreneur/Le sous-traitant étranger destinataire reconnaît que les obligations dont il doit s'acquitter en vertu du contrat s'ajoutent à toutes celles qui lui incombent en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L. C. 2000, ch.5, ou d'une loi similaire en vigueur dans une province ou un territoire du Canada. Si l'**entrepreneur/le sous-traitant** étranger destinataire estime que l'une ou l'autre des obligations du contrat l'empêche de s'acquitter de ses obligations en vertu de ces lois, il doit immédiatement informer l'autorité contractante de la disposition du contrat et de l'obligation de la loi qu'il considère comme contradictoires.

o) **Disposition des dossiers et remise des dossiers au Canada**

L'**entrepreneur ou le sous-traitant** étranger destinataire ne peut éliminer aucun dossier à moins que l'autorité contractante le lui demande. À la demande de l'autorité contractante, ou lorsque les travaux liés aux renseignements personnels sont terminés, le **contrat ou le contrat de sous-traitance** est terminé ou résilié, selon la première occurrence, l'**entrepreneur ou le sous-traitant** étranger destinataire doit retourner tous les dossiers (y compris les copies) à l'autorité contractante.

p) **Obligation juridique de divulguer les renseignements personnels**

Avant de divulguer tout renseignement personnel conformément à toute loi, à tout règlement ou toute ordonnance rendue par une cour de justice, un tribunal ou une entité administrative compétente, l'**entrepreneur ou le sous-traitant** étranger destinataire doit immédiatement informer l'autorité contractante afin de lui permettre de participer aux procédures pertinentes.

q) **Plaintes**

Le Canada et l'**entrepreneur/le sous-traitant** étranger destinataire conviennent de s'informer immédiatement et mutuellement de la réception d'une plainte en vertu de la *Loi sur l'accès à l'information*, de la *Loi sur la protection des renseignements personnels* ou de toute autre loi pertinente concernant les renseignements personnels. Les parties conviennent de s'échanger toute information nécessaire pour faciliter le règlement de la plainte et de s'informer immédiatement et mutuellement de son dénouement.

r) **Exception**

Les obligations énoncées dans ces conditions générales supplémentaires ne s'appliquent pas aux renseignements personnels qui sont déjà du domaine public, du moment qu'elles ne sont

pas devenues du domaine public, à la suite d'une faute ou d'une omission de l'entrepreneur ou de tout sous-traitant, agent ou représentant de l'entrepreneur ou de leurs employés.

71

7.19 Site ou locaux de l'entrepreneur nécessitant des mesures de protection

L'entrepreneur doit maintenir avec diligence des renseignements à jour liés à ses emplacements ou à ses locaux ou à ceux des personnes proposées où des mesures de protection sont requises pour l'exécution des travaux, aux adresses suivantes :

Numéro et nom de rue, numéro d'unité, de bureau ou d'appartement

Ville (province/territoire) / État

Code postal ou ZIP

Pays

L'agent de sécurité d'entreprise doit s'assurer, par l'intermédiaire du Programme de sécurité des contrats, que l'entrepreneur et les personnes proposées détiennent une habilitation de sécurité valide au niveau requis pour la protection des documents.

7.20 Sécurité physique et sécurité de l'information

Les exigences en matière de sécurité du Gouvernement du Canada requièrent que tout système informatique doit respecter pour protéger les renseignements personnels, la vie privée et/ou les biens gouvernementaux du Canada. L'entrepreneur doit mettre en œuvre des mesures de sécurité qui protégeront le système contenant des renseignements non classifiés, avec peu d'intégrité et de disponibilité. L'entrepreneur doit fournir l'accès et l'utilisation d'une solution qui protégera les citoyens canadiens et l'information et les actifs du Gouvernement du Canada en mettant en œuvre des contrôles de sécurité, des mesures et/ou des dispositifs à l'intérieur de la solution.

7.21 Base de paiement

a) **Phase 1 – Solution prototype :** Pour les travaux décrits à la phase 1 – Solution prototype de l'annexe A – Énoncé des travaux. En contrepartie du respect par l'entrepreneur de ses obligations en vertu du contrat, l'entrepreneur recevra un prix de lot ferme tout compris conformément à l'annexe B – Base de paiement, en dollars canadiens, droits de douane inclus, la taxe sur les produits et services ou la taxe de vente harmonisée est en sus, le cas échéant. Le prix de lot ferme tout compris comprend la livraison d'une solution prototype. Cette prestation comprend les droits d'utilisation, les octrois d'accès, la formation des utilisateurs, la documentation du logiciel, la garantie, ainsi que l'entretien et le soutien, les renonciations, les ententes de non-divulgation et tout autre lancement destiné au Canada aux fins de l'évaluation des capacités et de la convivialité (ÉCC). Le prix comprend jusqu'à 100 licences ou accès d'utilisateurs ou les deux, le cas échéant, pour utiliser simultanément la solution prototype à des fins d'évaluation de la capacité et de la convivialité pendant le contrat initial.

b) **Phase 1 - Test du prototype sur plateforme (PDP) (s'il y a lieu) :** Sur demande de l'autorité contractante pour les travaux décrits pour effectuer le test du prototype sur plateforme (PDP). En contrepartie du respect par l'entrepreneur de ses obligations en vertu du contrat, l'entrepreneur recevra un prix de lot ferme tout compris conformément à l'annexe B – Base de paiement, en dollars canadiens, droits de douane inclus, la taxe sur les produits et services ou la taxe de vente harmonisée est en sus, le cas échéant. Le prix de lot ferme tout compris comprend l'installation et l'intégration de la solution prototype sur le site Protégé B dans le

nuage loué par la GRC, les droits d'utilisation, les octrois d'accès, la documentation du logiciel, la garantie, l'entretien et le soutien, les renonciations, les accords de non-divulgation et tout autre lancement destiné au Canada aux fins de l'exécution du test de POP pour un maximum de 100 licences ou accès d'utilisateurs ou les deux, le cas échéant, permettant à ces utilisateurs d'utiliser simultanément la solution prototype.

c) **Option de la phase 2 – Solution :** Option de la phase 2 – Solution : Le Canada peut, à la seule discrétion, exercer l'option irrévocable de livrer la solution complète conformément à la phase 2 – Solution de l'annexe A – Énoncé des travaux. Si le Canada exerce cette option irrévocable, et que l'entrepreneur remplit de façon satisfaisante ses obligations en vertu du contrat, l'entrepreneur recevra un prix de lot ferme tout compris conformément à l'annexe B – Base de paiement, en dollars canadiens, droits de douane inclus, taxe sur les produits et services ou taxe de vente harmonisée en sus, le cas échéant. Le prix de lot ferme tout compris comprend, lorsqu'applicable, la livraison, l'installation, l'intégration et la configuration de la solution, ainsi que les services d'infrastructure de technologie de l'information accessoires et supplémentaires requis, la documentation logicielle, la garantie, la maintenance et le soutien, la formation pendant la période de mise en œuvre de la solution, les renonciations, les ententes de non-divulgation, les autres versions de la solution pour le Canada et toutes les licences ou les accès d'utilisateurs ou les deux, le cas échéant, pour un maximum de 2000 utilisateurs afin accéder à la solution et l'utiliser conformément au contrat.

d) **Option de licences d'utilisation supplémentaires ou d'accès d'utilisateur supplémentaires ou les deux, le cas échéant** : Le Canada peut, à la seule discrétion, exercer l'option irrévocable pour que l'entrepreneur fournisse des licences d'utilisation supplémentaires ou des accès d'utilisateurs supplémentaires ou les deux, le cas échéant. Si le Canada exerce cette option irrévocable, et que l'entrepreneur remplit de façon satisfaisante ses obligations en vertu du contrat, l'entrepreneur recevra un prix de lot ferme conformément à l'annexe B – Base de paiement, en dollars canadiens, droits de douane inclus, taxe sur les produits et services ou taxe de vente harmonisée en sus, le cas échéant.

e) **Services professionnels facultatifs fournis conformément à une autorisation de tâche avec un prix ferme :** Pour les services professionnels demandés par le Canada, conformément à une autorisation de tâche émise de manière valide et au fait que l'entrepreneur remplisse de façon satisfaisante ses obligations en vertu du contrat, le Canada paiera à l'entrepreneur le prix ferme par produit livrable (à l'exception des frais de déplacement et de subsistance), tel qu'il est établi dans l'autorisation de tâche, les taxes applicables en sus et tout produit livrable subséquent en conformité avec les honoraires quotidiens fermes établis à l'annexe B, Base de paiement. Les jours partiels seront calculés au prorata en se fondant sur les heures réelles travaillées, selon une journée de travail de 7,5 heures.

f) **Services de formation optionnels fournis conformément à une autorisation de tâche avec un prix ferme :** Pour les services de formation demandés par le Canada, conformément à une autorisation de tâche émise de manière valide et au fait que l'entrepreneur remplisse de façon satisfaisante ses obligations en vertu du contrat, le Canada paiera à l'entrepreneur le prix ferme (à l'exception des frais de déplacement et de subsistance), tel qu'il est établi dans l'autorisation de tâche, les taxes applicables en sus en conformité avec le prix ferme par lot établi à l'annexe B, Base de paiement.

g) **Services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant) fournis en vertu d'une autorisation de tâches avec un prix ferme** : Pour acquérir des services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant) demandés

par le Canada, conformément à une autorisation de tâches valablement délivrée et à l'exécution satisfaisante par l'entrepreneur de ses obligations en vertu du contrat, le Canada paiera à l'entrepreneur le prix ferme par produit livrable tel qu'indiqué dans l'autorisation de tâches, taxes applicables en sus, conformément aux prix de lot fermes indiqués à l'annexe B, Base de paiement. Toute période partielle de services de soutien sera calculée au prorata en fonction de l'année réelle de la période fournie sur une base de 365 jours par année.

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

(i) Tout déplacement doit être approuvé au préalable par l'autorité technique.

(ii) Tout paiement peut faire l'objet d'une vérification par le gouvernement.

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

j) **Limite de dépense – Services professionnels fournis conformément à une autorisation de tâche**

(i) La responsabilité totale du Canada à l'égard de l'entrepreneur aux termes du contrat pour toutes les autorisations de tâche (AT) accordées, y compris toutes les révisions apportées, ne doit pas dépasser la somme de ____ $ (*à insérer au moment de l'attribution du contrat*). Les droits de douane sont inclus, mais les taxes applicables sont en sus.

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

(iii) L'entrepreneur doit informer par écrit l'autorité contractante de l'augmentation nécessaire, dès que l'un ou l'autre des cas suivants se présente :

(1) lorsque 75 % de la somme est engagée;
(2) quatre (4) mois avant la date d'expiration du contrat;
(3) ou dès que l'entrepreneur juge que la somme est insuffisante pour l'achèvement des travaux requis dans le cadre des autorisations de tâches autorisées, y compris toutes révisions, selon la première de ces conditions à se présenter.

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

k) **Limite de dépense – Services de formation fournis conformément à une autorisation de tâche**

(i) La responsabilité totale du Canada à l'égard de l'entrepreneur aux termes du contrat pour toutes les autorisations de tâche (AT) accordées, y compris toutes les révisions

apportées, ne doit pas dépasser la somme de ____ $ (*à insérer au moment de l'attribution du contrat*). Les droits de douane sont inclus, mais les taxes applicables sont en sus.

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

(iii) L'entrepreneur doit informer par écrit l'autorité contractante de l'augmentation nécessaire, dès que l'un ou l'autre des cas suivants se présente :

i. lorsque 75 % de la somme est engagée;

ii. quatre (4) mois avant la date d'expiration du contrat;

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

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

l) **Limite de dépense – Services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant) fournis conformément à une autorisation de tâche**

(i) La responsabilité totale du Canada à l'égard de l'entrepreneur aux termes du contrat pour toutes les autorisations de tâche (AT) accordées, y compris toutes les révisions apportées, ne doit pas dépasser la somme de ____ $ (*à insérer au moment de l'attribution du contrat*). Les droits de douane sont inclus, mais les taxes applicables sont en sus.

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

(iii) L'entrepreneur doit informer par écrit l'autorité contractante de l'augmentation nécessaire, dès que l'un ou l'autre des cas suivants se présente :

(1) lorsque 75 % de la somme est engagée;

(2) quatre (4) mois avant la date d'expiration du contrat;

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

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

7.22 Modalités de paiement

a) **Paiement unique – Phase 1 – Prototype de solution** (Référence Tableau 1 de l'annexe B, Base de paiement)

Le Canada paiera l´entrepreneur lorsque les travaux liés au Prototype de solution de la Phase 1 seront exécutés et livrés conformément aux dispositions de paiement du contrat si :

(i) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis selon les instructions de facturation prévues au contrat;
(ii) tous ces documents ont été vérifiés par le Canada; et
(iii) les travaux exécutés ont été acceptés par le Canada.

b) **Paiement unique – Phase 1 – Test de prototype sur plateforme** (Référence Tableau 2 de l'annexe B, Base de paiement)

Le Canada paiera l´entrepreneur lorsque les travaux liés au Test de prototype sur plateforme seront exécutés et livrés conformément aux dispositions de paiement du contrat si :

(iv) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis selon les instructions de facturation prévues au contrat;
(v) tous ces documents ont été vérifiés par le Canada; et
(vi) les travaux exécutés ont été acceptés par le Canada.

c) **Paiement progressif – Assujettis à une retenue – Option Phase 2 Mise en œuvre de la Solution, le cas échéant** (Référence Tableau 3 et Tableau des paiements d'étape – Soutien à la mise en œuvre de l'annexe B, Base de paiement)

À son unique discrétion, le Canada peut exercer l'option irrévocable selon laquelle l'entrepreneur exécutera les travaux conformément à l'article 3 de la Phase 2 – Solution de l'annexe A – Énoncé des travaux. Si le Canada exerce cette option irrévocable, il effectuera des paiements progressifs à l'entrepreneur conformément au calendrier d'étapes détaillé à l'annexe B – Base de paiement du contrat et aux dispositions de paiement du contrat, jusqu'à concurrence de 90 % du montant réclamé et approuvé par le Canada si :

(i) une demande de paiement exacte et complète effectuée au moyen du formulaire PWGSCTPSGC 1111, Demande de paiement progressif, et tout autre document exigé par le contrat ont été présentés conformément aux instructions relatives à la facturation fournies dans le contrat;
(ii) le montant total de tous les paiements d'étape effectués par le Canada ne dépasse pas quatre-vingt-dix pour cent (90 %) du montant total à verser aux termes du contrat;
(iii) toutes les attestations demandées sur le formulaire PWGSC-TPSGC 1111 ont été signées par les représentants autorisés concernés; et
(iv) tous les travaux associés à l'étape et, selon le cas, les produits livrables, sont terminés et ont été acceptés par le Canada.

Le solde du montant dû sera payé conformément aux dispositions de paiement du contrat lorsque tous les travaux exigés au contrat auront été exécutés et livrés si les travaux ont été acceptés par le Canada et qu'une demande finale de paiement est présentée.

d) **Paiement mensuel – Option de licences d'utilisation supplémentaires (le cas échéant) ou d'accès pour les utilisateurs supplémentaires (le cas échéant) ou les deux (le cas échéant)** (Référence Tableau 4, Tableau 5 A, Tableau 5B de l'annexe B, Base de paiement)

Le Canada peut, la seule discrétion, exercer l'option irrévocable pour que l'entrepreneur fournisse des licences d'utilisation supplémentaires ou des accès d'utilisateur supplémentaires, ou les deux, selon le cas. Si le Canada exerce cette option irrévocable, le Canada paiera mensuellement l'entrepreneur les frais liés aux licences d'utilisation supplémentaires ou accès d'utilisateur supplémentaires, ou les deux (le cas échéant) pendant le mois visé par la facture conformément aux dispositions de paiement du Contrat si :

(i) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis selon les instructions de facturation prévues au contrat;
(ii) tous ces documents ont été vérifiés par le Canada; et
(iii) les travaux exécutés ont été acceptés par le Canada.

e) **Paiement mensuel – Services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant) par une autorisation de tâche et assortis d'un prix ferme** (Référence Table 6 de of Annexe B, Base de paiement)

Le Canada peut, la seule discrétion, exercer l'option irrévocable pour que l'entrepreneur fournisse des services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant). Si le Canada exerce cette option irrévocable, le Canada paiera mensuellement l'entrepreneur les services de maintenance et de soutien optionnels de la solution (le cas échéant) ou services d'hébergement et de soutien optionnels connexes à l'hébergement de la SNC (le cas échéant) ou les deux (le cas échéant) pendant le mois visé par la facture conformément aux dispositions de paiement du contrat si :

(i) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis selon les instructions de facturation prévues au contrat;
(ii) tous ces documents ont été vérifiés par le Canada; et
(iii) les travaux exécutés ont été acceptés par le Canada.

f) **Paiement mensuel – Services professionnels facultatifs visés par une autorisation de tâche et assortis d'un prix ferme**

Le Canada paiera l'entrepreneur chaque mois pour les travaux effectués pendant le mois visé par la facture conformément aux dispositions de paiement du contrat si :

(i) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis selon les instructions de facturation prévues au contrat;
(ii) tous ces documents ont été vérifiés par le Canada;
(iii) les travaux exécutés ont été acceptés par le Canada.

g) **Paiement mensuel – Services de formation optionnels visés par une autorisation de tâche et assortis d'un prix ferme** (Référence Tableau 8 de l'Annexe B, Base de paiement)

Le Canada paiera l'entrepreneur chaque mois pour les travaux effectués pendant le mois visé par la facture conformément aux dispositions de paiement du contrat si :

(i) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis selon les instructions de facturation prévues au contrat;
(ii) tous ces documents ont été vérifiés par le Canada;
(iii) les travaux exécutés ont été acceptés par le Canada.

7.23 Facturation

a) **Présentation des factures.** L'entrepreneur doit présenter des factures pour les services et la livraison des travaux, s'il y a lieu.

b) **Exigences relatives à la facture.** Les factures doivent être soumises au nom de l'entrepreneur et contenir :

(i) la date, le nom et l'adresse du ministère client, les numéros d'articles ou de référence, les livrables ou la description des travaux, le numéro du contrat, le numéro de référence du client (NRC), le numéro d'entreprise – approvisionnement (NEA) et le ou les codes financiers;

(ii) des renseignements sur les dépenses (comme le nom des articles et leur quantité, l'unité de distribution, le prix unitaire, les tarifs horaires fermes, le niveau d'effort et les sous-traitances, selon le cas) conformément à la base de paiement, excluant les taxes applicables.

(iii) déduction pour retenue, le cas échéant; et prolongation des totaux, le cas échéant.

Les taxes applicables doivent être indiquées séparément dans toutes les factures, ainsi que les numéros d'inscription correspondant émis par les autorités fiscales. Tous les articles détaxés, exonérés ou auxquels les taxes applicables ne s'appliquent pas doivent être identifiés comme tels sur toutes les factures.

c) **Instructions de facturation - Libération de la retenue et solde du paiement**

(i) L'entrepreneur doit présenter les factures conformément à la section intitulée « Présentation des factures » des conditions générales. Les factures ne peuvent pas être soumises tant que tous les travaux indiqués dans la facture ne sont pas terminés.

Outre les exigences des conditions générales, chaque facture doit être appuyée par :

i. tous les documents applicables à la libération de la retenue ainsi que tous les autres documents requis en vertu du contrat; et
ii. tous les certificats d'inspection relatifs aux biens et/ou aux services qui font l'objet de la facture, fournis sous forme de copie PDF numérisée avec les signatures officielles des autorités de certification désignées et non seulement les noms imprimés.

(ii) Conformément à l'article du contrat sur les paiements d'étape, tout solde du montant à payer sera payé conformément aux dispositions de paiement du contrat et selon les conditions suivantes : achèvement et livraison de tous les travaux requis en vertu de chaque autorisation de tâche du contrat, réalisation de tout rajustement requis tel que décrit dans la « Base de paiement », acceptation des travaux concernés par le Canada et présentation d'une facture finale pour le paiement requis.

(iii) Les factures doivent être distribuées comme suit :
i. L'original et une (1) copie doivent être envoyés à l'autorité technique, identifiée dans la section intitulée « Autorités » du contrat, pour vérification et paiement.
ii. Une (1) copie doit être transmise à l'autorité contractante désignée à la section intitulée « Autorités » du contrat.

7.24 Taxes

a) **Paiement des taxes.** Les taxes applicables seront payées par le Canada conformément aux dispositions de l'article sur la présentation des factures. Il incombe à l'entrepreneur de facturer les taxes applicables selon le taux approprié, conformément aux lois en vigueur. L'entrepreneur accepte de remettre aux autorités fiscales appropriées les sommes acquittées ou exigibles au titre de taxes applicables.

b) **Retenue pour les non-résidents.** Le Canada doit retenir 15 % du montant à payer à l'entrepreneur pour des services rendus au Canada si l'entrepreneur n'est pas un résident du Canada, à moins que ce dernier obtienne une exonération valide de l'Agence du revenu du Canada. Le montant retenu sera conservé dans un compte pour l'entrepreneur à l'égard de toute dette fiscale exigible par le Canada.

c) **Entrepreneur établi à l'étranger.** À moins d'indication contraire dans le contrat, le prix ne comprend aucune taxe fédérale d'accise, taxe locale ou d'État, de vente ou d'utilisation, aucune autre taxe de nature semblable, ni autre taxe canadienne, quelle qu'elle soit. Par contre, le prix inclut toutes les autres taxes. Si les travaux sont normalement assujettis à la taxe d'accise fédérale, le Canada fournira à l'entrepreneur, sur demande, un certificat d'exonération de cette taxe selon la forme prescrite par le règlement fédéral.

d) Le Canada fournira à l'entrepreneur les preuves d'exportation qui peuvent être demandées par les autorités fiscales. Si le Canada omet de le faire, et qu'en conséquence l'entrepreneur doit payer la taxe fédérale d'accise, le Canada remboursera l'entrepreneur si celui-ci prend les mesures que le Canada peut exiger pour recouvrer tout paiement effectué par l'entrepreneur. L'entrepreneur doit rembourser au Canada tout montant ainsi recouvré.

e) **Attestation de factures.** L'entrepreneur atteste que la facture correspond aux travaux qui ont été livrés et qu'elle est conforme au marché d'acquisition.

f) **Période de paiement.** Le Canada paiera le montant non contesté de la facture de l'entrepreneur dans les 30 jours suivant sa réception. Dans l'éventualité où une facture n'est pas dans une forme et un contenu acceptables, le Canada en avisera l'entrepreneur et le délai de paiement de 30 jours débutera à la réception d'une facture conforme.

g) **Intérêts sur les paiements en retard.** Le Canada versera à l'entrepreneur des intérêts simples, au taux moyen majoré de 3 % par an, sur toute somme en souffrance, à partir du premier jour où la somme est en souffrance jusqu'au jour qui précède la date de paiement inclusivement, à condition que le Canada soit responsable du retard de paiement à l'entrepreneur. Le Canada ne versera pas d'intérêts sur les paiements anticipés qui sont en souffrance.

h) Paiement électronique des factures – Contrat

L'entrepreneur accepte d'être payé à l'aide des instruments de paiement électronique suivants :

(i) carte d'achat Visa:

(ii) carte d'achat MasterCard;

(iii) dépôt direct (national et international);

(iv) échange de données informatisé (EDI);

(v) virement télégraphique (international seulement);

(vi) système de transfert de paiements de grande valeur (plus de 25 millions de dollars).

7.25 Attestations et renseignements supplémentaires

À moins d'indications contraires, le respect continu des attestations fournies par l'entrepreneur dans sa soumission ou préalablement à l'attribution du contrat, ainsi que la coopération constante quant aux renseignements supplémentaires à fournir, sont des conditions du contrat, et leur non-respect constituera un manquement aux obligations de la part de l'entrepreneur dans le cadre du contrat. Les attestations pourront faire l'objet d'une vérification par le Canada pendant toute la durée du contrat.

7.26 Programme de contrats fédéraux pour l'équité en matière d'emploi – Manquement de la part de l'entrepreneur

L'entrepreneur comprend et convient que l'entente de mise en œuvre de l'équité en matière d'emploi conclue avec le Programme du travail d'Emploi et Développement social Canada doit demeurer valide pendant toute la durée du contrat. Si cette entente devient invalide, le nom de l'entrepreneur sera ajouté à la « Liste d'admissibilité limitée à soumissionner au Programme de contrats fédéraux ». L'imposition d'une telle sanction par EDSC aura pour effet de placer l'entrepreneur en situation de non-conformité au regard des conditions du contrat.

7.27 Exigences relatives à l'assurance

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

7.28 Attestation de prix

L'entrepreneur atteste que le prix proposé n'est pas supérieur au plus bas prix demandé à tout autre client, y compris à son meilleur client, pour une qualité et une quantité semblables de biens, de services ou les deux.

7.29 Limitation de responsabilité

Sauf indiqué expressément dans le paragraphe b), l'entrepreneur est responsable de tous les dommages qu'il cause durant l'exécution ou par manque d'exécution du contrat en relation avec :

a) tout acte ou omission dans le cadre du contrat qui affecte les biens réels ou tangibles que ce soient possédés, détenus ou occupés par le Canada;

b) le manquement à l'obligation de confidentialité par l'entrepreneur en vertu du contrat, mais cette limitation ne s'applique pas à la divulgation de secret commerciaux du Canada ou de tiers en relation avec la technologie informatique;

c) toute charge ou tout privilège sur toute portion des travaux dans le cadre du contrat, qui n'incluent pas les réclamations ou charges relatives aux droits de propriété intellectuelle;

d) le manquement aux obligations de garantie par l'entrepreneur.

Cependant, l'entrepreneur n'est pas responsable envers le Canada des dommages indirects, particuliers ou consécutifs causés par les paragraphes a) à d) ci-dessus.

En ce qui concerne les dommages directs liés à la violation par l'entrepreneur de ses obligations de garantie, la responsabilité maximale de l'entrepreneur envers le Canada est le coût estimatif total du contrat (c'est-à-dire le montant en dollars indiqué sur la première page du contrat dans le bloc intitulé « **Coût estimatif total** »). Tous les dommages directs non énumérés ci-dessus qui ne sont pas liés à une violation de garantie sont assujettis à un maximum de 0,25 fois le coût total estimatif ou 1 M $, selon le montant le plus élevé.

Si les dossiers ou les données du Canada sont endommagés à la suite d'une négligence ou d'un acte délibéré de l'entrepreneur, la seule responsabilité de l'entrepreneur consiste à rétablir à ses frais les dossiers et les données du Canada en utilisant la copie de sauvegarde la plus récente conservée par le Canada. Il incombe au Canada de sauvegarder adéquatement ses dossiers et ses données.

Les limitations ci-dessus ne s'appliquent pas aux dommages basés sur la perte de vie ou la blessure corporelle, ou les réclamations basées sur la violation des droits de propriété intellectuelle.

7.30 Dispositions générales

a) **Lois applicables**. Le présent contrat sera interprété et régi selon les lois en vigueur en Ontario.

b) **Survie**. Les obligations des parties concernant la confidentialité, les déclarations et les garanties prévues dans le contrat ainsi que les dispositions qu'il est raisonnable de présumer, en raison de la nature des droits et des obligations, qu'elles devraient rester en vigueur, demeurent applicables malgré l'expiration du contrat ou sa résiliation.

c) **Divisibilité.** Si une quelconque disposition du présent contrat est déclarée inapplicable par un tribunal compétent, le reste du présent contrat restera en vigueur.

d) **Renonciation.** Le fait de ne pas faire valoir l'un des droits prévus au présent contrat ou de négliger de le faire ne sera pas considéré comme une renonciation aux droits de cette partie.

e) **Aucun pot-de-vin.** L'entrepreneur déclare qu'aucun pot-de-vin, cadeau, bénéfice ou autre avantage n'a été ni ne sera payé, donné, promis ou offert, directement ou indirectement, à un représentant ou à un employé du Canada ni à un membre de sa famille, en vue d'exercer une influence sur l'attribution ou la gestion du contrat.

f) **Honoraires conditionnels.** L'entrepreneur atteste qu'il n'a pas versé ni convenu de verser, directement ou indirectement, et convient de ne pas verser, directement ou indirectement, des honoraires conditionnels en rapport avec la soumission, la négociation ou l'obtention du contrat

à toute personne autre qu'un employé de l'entrepreneur remplissant les fonctions habituelles liées à son poste. Dans le présent article, « honoraires conditionnels » signifie tout paiement ou autre forme de rémunération qui est subordonnée au degré de succès ou calculée en fonction du degré de succès obtenu dans la sollicitation, la négociation ou l'obtention du contrat, et « personne » signifie tout particulier qui est tenu de fournir au registraire une déclaration en vertu de l'article 5 de la *Loi sur le lobbying*, 1985, ch. 44 (4e suppl.).

g) **Sanctions internationales**.

(i) Les Canadiens et les Canadiennes et les ressortissants canadiens à l'étranger sont liés par les sanctions économiques imposées par le Canada. En conséquence, le gouvernement du Canada ne peut accepter la livraison d'aucun bien ou service provenant, directement ou indirectement, d'un ou plusieurs pays ou personnes assujettis à des sanctions économiques.

(ii) Le fournisseur ne doit livrer au gouvernement du Canada aucun bien ni aucun service assujetti à des sanctions économiques.

L'entrepreneur doit se conformer aux modifications apportées aux règlements imposés pendant la période du contrat. L'entrepreneur doit immédiatement aviser le Canada s'il est dans l'impossibilité d'exécuter le contrat à la suite de l'imposition de sanctions à un pays ou à une personne ou de l'ajout de biens ou de services à la liste des biens ou des services sanctionnés. Si les parties ne peuvent alors s'entendre sur un plan de redressement, le contrat sera résilié.

h) **Dispositions relatives à l'intégrité – Contrat**. La *Politique d'inadmissibilité et de suspension* (la « Politique ») et toutes les directives incorporées par renvoi à l'invitation à soumissionner à sa date de clôture sont intégrées au contrat et en font partie intégrante. L'entrepreneur doit se conformer aux dispositions de la politique et des directives; celles-ci se trouvent sur le site internet de Travaux publics et Services gouvernement Canada sous *Politique d'inadmissibilité et de suspension*.

i) **Code de conduite pour l'approvisionnement – Contrat**. L'entrepreneur accepte de se conformer au *Code de conduite pour l'approvisionnement* et d'être lié par celui-ci pendant la durée du contrat.

j) **Code régissant les conflits d'intérêts et code de valeurs et d'éthique de la fonction publique**. L'entrepreneur reconnaît que les personnes qui sont assujetties aux dispositions de la *Loi sur les conflits d'intérêts*, 2006, ch. 9, art. 2, du Code régissant la conduite des titulaires de charge publique en ce qui concerne les conflits d'intérêts et l'après-mandat, du Code de valeurs et d'éthique de la fonction publique ou tout autre code de valeur et d'éthique en vigueur au sein d'organismes spécifiques ne peuvent bénéficier directement du contrat.

7.31 Autorités

a) **Autorité contractante**

Pour ce contrat, l'autorité contractante est :

Nom : **Jean-Claude Labossière**
Titre : Spécialiste en approvisionnements
Organisation : Services publics et Approvisionnement Canada – Direction générale des approvisionnements
Direction : Direction de l'approvisionnement d'applications et de logiciels
Adresse : 10, rue Wellington, Gatineau (Québec) K1A 0S5
Téléphone : 613-858-7359
Adresse de courriel : Jean-Claude.Labossiere@tpsgc-pwgsc.gc.ca

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

b) **Autorité technique** – Gendarmerie Royale du Canada

Ces renseignements seront ajoutés au moment de l'attribution du contrat.

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____
Téléphone : _____
Télécopieur : _____
Adresse de courriel : _____

L'autorité technique représente le ministère ou organisme pour lesquels les travaux sont exécutés dans le cadre du contrat. Il est responsable de toutes les questions liées au contenu technique des travaux prévus dans le contrat. Il est possible de discuter des questions techniques avec l'autorité technique; cependant, celle-ci ne peut pas autoriser les changements à apporter à la portée des travaux. De tels changements peuvent être effectués uniquement au moyen d'une modification au contrat apportée par l'autorité contractante.

c) **Autorité de sécurité de la chaîne d'approvisionnement (à insérer au moment de l'attribution du Contrat**

Nom :

Titre :

Téléphone :

Adresse électronique :

L'autorité de sécurité de la chaîne d'approvisionnement est le représentant de Services partagés Canada (SPC) et elle est responsable de toutes les questions liées au processus continu d'intégrité de la chaîne d'approvisionnement en vertu du présent contrat. Ni l'autorité contractante ni l'autorité technique n'ont le pouvoir de fournir des conseils ou d'autoriser la divulgation de renseignements liés au processus d'intégrité de la chaîne d'approvisionnement. L'autorité de sécurité de la chaîne d'approvisionnement demeure responsable de tous les autres aspects liés à la sécurité.

7.32 Divulgation proactive de contrats conclus avec d'anciens fonctionnaires

En fournissant des renseignements sur son statut d'ancien fonctionnaire touchant une pension en vertu de la *Loi sur la pension de la fonction publique* (LPFP), l'entrepreneur a convenu que ces renseignements seront affichés sur les sites Web ministériels, conformément à l'Avis sur la politique sur les marchés 2012-2 du Secrétariat du Conseil du Trésor du Canada.

7.33 Priorité des documents

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

a) les articles du présent accord, y compris les clauses du guide des CCUA qui y sont intégrées par renvoi;

b) les conditions générales 2035 (2020-05-28) - besoins de services plus complexes;

c) les conditions générales 2030 (2020-05-28) - besoins de biens plus complexes;

d) les conditions générales supplémentaires, dans l'ordre suivant :

(i) 4008, (2008-12-12) Renseignements personnels;

(ii) 4006, (2010-08-16) L'entrepreneur détient les droits de propriété intellectuelle sur les renseignements originaux;

(iii) 4003, (2010-08-16) Logiciels sous licence; and

(iv) 4004, (2013-04-25) Services de maintenance et de soutien des logiciels sous licence.

e) Annexe A – Énoncé des travaux;

f) Annexe B – Base de paiement;

g) Annexe C – Liste de vérification des exigences en matière de sécurité;

h) Annexe D – Définitions et interprétations;

i) Annexe E – Obligations relatives à la vie privée;

j) Annexe F – Intégrité de la chaine d'approvisionnement;

k) les autorisations de tâches signées ainsi que les attestations nécessaires;

l) Annexe G – Formulaires d'autorisation de tâche;

m) Annexe H – Paiements progressifs;

n) Annexe I – Formulaires du soumissionnaire;

o) la soumission de l'entrepreneur datée du ____ (*insérer la date de la soumission*)

7.34 Ressortissants étrangers (entrepreneur canadien)

a) Guide des CCUA clause A2000C (2006-06-16) Ressortissants étrangers (entrepreneur canadien).

Note aux soumissionnaires : La présente clause ou celle qui suit, selon ce qui s'applique (selon que le soumissionnaire retenu est un entrepreneur canadien ou un entrepreneur étranger), sera incluse dans tout contrat subséquent.

7.35 Ressortissants étrangers (entrepreneur étranger)

a) Guide des CCUA clause A2001C (2006-06-16) Ressortissants étrangers (entrepreneur étranger).

7.36 Entrepreneur - coentreprise

a) L'entrepreneur confirme que le nom de la coentreprise est _____ et que cette dernière est constituée des membres suivants :

b) En ce qui a trait aux rapports entre les membres de cette coentreprise, chacun d'eux convient, déclare et garantit (selon le cas) que :

(i) _____ a été nommé en tant que « membre représentant » de la coentreprise et est pleinement habilité à intervenir à titre de mandataire de chacun des membres de cette coentreprise concernant toutes les questions se rapportant au présent contrat;

(ii) en signifiant les avis et préavis au membre représentant, le Canada sera réputé les avoir signifiés également à tous les membres de cette coentreprise;

(iii) toutes les sommes versées au membre représentant en vertu du contrat seront réputées l'avoir été à tous les membres de la coentreprise.

c) Tous les membres de la coentreprise acceptent que le Canada puisse, à sa discrétion, résilier le contrat en cas de différend entre les membres si, de l'avis du Canada, ce différend influe de quelque façon sur l'exécution des travaux.

d) Tous les membres de la coentreprise sont conjointement et individuellement ou solidairement responsables de l'exécution du contrat en entier.

e) L'entrepreneur reconnaît que toute modification apportée à la composition de la coentreprise (c.-à-d., un changement dans le nombre de ses membres ou le remplacement d'un membre par une autre) constitue une affectation et est assujetti aux dispositions des conditions générales du contrat.

f) L'entrepreneur reconnaît que toutes les exigences du marché en matière de sécurité et de marchandises contrôlées s'appliquent également à chaque membre de la coentreprise.

Remarque à l'intention des soumissionnaires : *Le présent article sera supprimé si le soumissionnaire auquel on attribue le contrat n'est pas une coentreprise. Si l'entrepreneur est une coentreprise, cette clause sera complétée avec l'information présentée dans la soumission.*

DEMANDE DE SOUMISSIONS

ANNEXES

SOLUTION NATIONALE EN MATIÈRE DE CYBERCRIMINALITÉ POUR LA GENDARMERIE ROYALE DU CANADA

Table des matières

CETTE PAGE EST VOLONTAIREMENT VIDE

ANNEXE A

ÉNONCÉ DES TRAVAUX (EDT)

SOLUTION NATIONALE EN MATIÈRE DE CYBERCRIMINALITÉ

TABLE DES MATIÈRES

ANNEXE A

Liste des figures

Liste des tableaux

1. Introduction

1.1 Titre

a) Solution nationale en matière de cybercriminalité (SNC), ci-après la « solution ».

1.2 Contexte

a) En 2015, le premier ministre du Canada a demandé au ministre de la Sécurité publique et de la Protection civile de diriger « un examen des mesures en place pour assurer la protection des Canadiens et des infrastructures essentielles du Canada contre les cybermenaces » (l'examen de la cybersécurité). L'examen de la cybersécurité comprenait des consultations publiques et auprès des intervenants en 2016 et un processus d'élaboration de politiques interministérielles en 2016 et 2017. Selon les conclusions de l'examen de la cybersécurité, le Canada doit se doter d'un mécanisme national de coordination des opérations policières contre les cybercriminels ainsi que d'un mécanisme national permettant aux Canadiens et aux entreprises de signaler les cybercrimes à la police (entre autres initiatives).

b) La police, au Canada comme à l'étranger, fait face à des cybercrimes semblables, et cette similitude des activités criminelles internationales exige une coordination nationale et multilatérale. Cependant, la communauté policière du Canada a besoin d'une organisation qui assure une coordination nationale en matière de lutte contre la cybercriminalité qui peut agir grâce à un solide système de gestion de l'information/technologie de l'information (GI/TI) propre à la cybercriminalité pour établir des liens, coordonner les efforts d'enquête au pays et à l'étranger et évaluer les répercussions économiques et sociales de la cybercriminalité en général. Le fait de ne pas répondre à ce besoin fait en sorte que des enquêtes n'ont pas lieu et crée des risques ainsi qu'un dédoublement des efforts.

c) Le signalement des crimes est essentiel aux enquêtes, à la protection des victimes et à la compréhension et à la prévention des crimes. Ceci est vrai tant pour la cybercriminalité que les fraudes. Les technologies numériques favorisent de plus en plus les fraudes traditionnelles (« commettre sous une nouvelle forme des crimes qui existaient déjà »), et la limite entre une fraude traditionnelle et un cybercrime est souvent floue. Tandis que les victimes de crimes traditionnels localisés peuvent signaler de telles activités à la police locale, la façon de signaler des cybercrimes est moins évidente, ce qui crée de la confusion.

d) Actuellement, il n'existe aucun système national permettant aux Canadiens et aux entreprises de signaler facilement un cybercrime à la police ou permettant aux services de police d'accéder aux rapports et aux analyses concernant les victimes. Le fait de ne pas répondre à ce besoin nuit aux enquêtes, aux macroanalyses, à la détermination des menaces et à un effort coordonné de la police pour comprendre la cybercriminalité et y répondre. Afin d'améliorer les signalements publics, la Gendarmerie royale du Canada (GRC) établira un système qui recevra les signalements de cybercriminalité et de fraude.

e) Ces lacunes – l'absence d'une organisation de coordination de lutte contre la cybercriminalité et l'absence de mécanisme national de signalement public des cybercrimes – ont été soulevées par plusieurs intervenants durant les consultations sur l'examen de la cybersécurité. En réponse, la GRC a créé le Groupe national de coordination contre la cybercriminalité (GNCC), qui sera entièrement opérationnel grâce à la nouvelle solution en matière de cybercriminalité.

1.3 Aperçu

a) Le mandat du GNCC est de permettre aux organismes d'application de la loi canadiens de réduire la menace, le nombre de victimes et les répercussions de la cybercriminalité au Canada.

b) Le GNCC :

i) coordonnera les opérations de lutte contre la cybercriminalité des organismes canadiens d'application de la loi et collaborera avec des partenaires internationaux;

ii) fournira des conseils et directives en matière d'enquête numérique aux services de police canadiens;

iii) produira du renseignement exploitable sur la cybercriminalité;

iv) établira un mécanisme national de signalement public qui permettra aux particuliers et aux entreprises du Canada de signaler les cybercrimes et les fraudes aux organismes d'application de la loi;

v) échangera des renseignements sur la cybercriminalité avec les services de police;

vi) cherchera des liens entre divers incidents de cybercriminalité distincts;

vii) contribuera à faire en sorte que plusieurs services de police ne fassent pas double emploi en enquêtant sur le même crime ou le même suspect chacun de leur côté.

1.4 Objectifs

a) Le GNCC doit disposer d'une solution nationale en matière de cybersécurité à l'avant-garde et de pointe afin de réaliser son mandat.

b) La solution doit :

i) permettre et soutenir l'échange réciproque sécurisé de demandes et de renseignements concernant la cybercriminalité avec les partenaires chargés de l'application de la loi (y compris, mais sans s'y limiter, les organismes nationaux et internationaux d'application de la loi et les organismes fédéraux) par l'entremise du Portail des partenaires et des policiers (P3) ainsi que d'autres moyens traditionnels, y compris mais sans s'y limiter, par courriel;

ii) soutenir l'échange de volumes importants de données structurées, semi-structurées et non structurées;

iii) fournir les capacités indiquées à l'Appendice C – Modèle de capacité opérationnelle de la SNC;

iv) fournir des capacités de gestion de cas, y compris recevoir, saisir, analyser, enrichir, corréler, évaluer et harmoniser les renseignements et les intégrer au sein de l'écosystème de la solution pour lancer de nouvelles enquêtes ou approfondir celles en cours;

v) fournir des capacités pour harmoniser et coordonner les efforts en matière de renseignement sur la cybercriminalité et la fraude dans l'ensemble de la communauté canadienne d'application de la loi ainsi qu'avec les organisations fédérales et internationales;

vi) offrir aux utilisateurs la capacité d'analyser les données afin de générer du renseignement et d'appuyer la prise de décisions;

vii) fournir une visualisation des données pour appuyer les conclusions et les déductions;

viii) offrir des fonctions avancées d'exploration de données pour aider les utilisateurs du GNCC à analyser les données non structurées, semi-structurées et structurées;

ix) fournir aux partenaires de la lutte contre la cybercriminalité des conseils, des outils et une orientation en matière d'enquête et de technique, et ce, directement et par l'entremise d'une base de connaissances en ligne au moyen du P3;

x) faciliter la détermination des échantillons de logiciels malveillants provenant des organismes canadiens d'application de la loi en les comparant à des bibliothèques de logiciels malveillants nationales ou internationales sélectionnées afin d'appuyer les efforts en matière de renseignement et d'enquêtes;

xi) fournir des capacités pour la gestion active des initiatives de collaboration et des partenariats avec le secteur privé et les autres ministères.

c) Les travaux seront réalisés conformément aux deux (2) phases décrites ci-dessous. L'entrepreneur doit, dans le cadre des travaux de la phase 1, mettre au point et livrer un prototype de solution dans un délai fixé conformément aux travaux de la phase 1 décrits à l'annexe A – Énoncé des travaux et aux critères d'évaluation des capacités et de la convivialité (ECC) de l'appendice A de l'annexe A – Énoncé des travaux. À la fin des travaux de la phase 1 et au terme d'une évaluation des solutions prototypes par le gouvernement du Canada, le gouvernement du Canada exercera, à sa discrétion exclusive, l'option irrévocable pour l'entrepreneur de réaliser les travaux et de livrer la solution complète conformément à la phase 2 de l'annexe A – Énoncé des travaux.

1.5 Exclus de la portée

a) La GRC élabore actuellement un site Web de signalement destiné au public. La conception du site Web est exclue de la portée du présent EDT. Les détails sur le site Web de signalement destiné au public sont inclus dans le présent EDT pour fournir à l'entrepreneur le contexte lié à un flux principal de rapports sur la cybercriminalité vers la solution.

b) La GRC agit seulement à titre de courtier pour les demandes de correspondance des logiciels malveillants. Elle n'effectue pas d'analyse détaillée des logiciels malveillants. Par conséquent, l'analyse des logiciels malveillants est exclue de la portée de la solution.

2. Phase 1 – Solution prototype

2.1 Portée des travaux

a) La portée des travaux relatifs à la solution prototype inclut la planification, la conception, le développement, la configuration, les essais et la livraison d'une solution prototype de qualité, hébergée dans le nuage et fonctionnelle prenant en charge jusqu'à cent (100) utilisateurs, conformément aux exigences techniques et fonctionnelles décrites dans les présentes.

2.2 Exigences

a) L'entrepreneur doit développer et livrer une solution prototype dans le nuage pouvant comprendre n'importe quelle combinaison de logiciels commerciaux standards, de logiciels sur mesure ou de logiciels ouverts, conformément aux exigences décrites à l'Appendice A – Évaluation des capacités et de la convivialité (ECC). L'interopérabilité et les points d'intégration entre les composantes de la solution prototype doivent être transparents pour l'utilisateur.

b) La configuration subséquente de la solution prototype de l'entrepreneur doit fournir au gouvernement du Canada une application intégrée qui prend en charge toutes les capacités et exigences décrites dans les scénarios d'utilisation détaillés à l'Appendice A – Évaluation des capacités et de la convivialité (ECC), en particulier :

   i) Scénario d'utilisation n° 1 – Demande de service d'un partenaire;

   ii) Scénario d'utilisation n° 2 – Municipalité touchée par un rançongiciel – Coordination et assistance;

   iii) Scénario d'utilisation n° 3 – Demande de partenaires concernant des conseils et une orientation en matière numérique;

   iv) Scénario d'utilisation n° 4 – Analytique

   v) Scénario d'utilisation n° 5 – Intégration du signalement public.

c) D'autres détails sur le contenu de chaque scénario sont décrits à l'Appendice A – Évaluation des capacités et de la convivialité (ECC).

2.3 Sécurité du prototype

a) En cas d'atteinte à la sécurité ayant une incidence sur la sécurité du prototype ou ayant le potentiel de compromettre le Canada ou ses clients de tout autre ordre de gouvernement, l'entrepreneur doit informer le Canada qu'une atteinte à la sécurité s'est produite. Le gouvernement du Canada précisera le délai dans lequel le risque doit être traité dans le rapport connexe sur l'atténuation des vulnérabilités.

b) L'entrepreneur doit conserver les rapports sur les atteintes à la sécurité, les transactions et les journaux de vérification, les rapports d'incident d'alarme et les rapports connexes de l'année en cours et des trois (3) années précédentes et doit obtenir l'autorisation écrite du gouvernement du Canada avant de détruire tout rapport datant de plus de deux (2) ans.

c) L'entrepreneur doit fournir les enregistrements de vérification de sécurité au gouvernement du Canada dans les dix (10) jours ouvrables après que l'État en aura fait la demande.

2.4 Évaluation des capacités et de la convivialité

a) Le gouvernement du Canada effectuera une évaluation des capacités et de la convivialité (ECC) des produits livrables de la solution prototype, conformément aux procédures et critères d'évaluation définis à l'Appendice A – Évaluation des capacités et de la convivialité (ECC).

2.5 Test de prototype sur plateforme

Le Canada peut effectuer, à sa seule discrétion, un essai de prototype sur plateforme (POP) en utilisant la solution prototype proposée par l'entrepreneur le mieux classé (identifié après l'évaluation des capacités et de la convivialité (ECC).

a) Si la solution est fournie dans l'espace infonuagique protégé B de la GRC ou au moyen d'un modèle hybride, le Canada effectuera un test de prototype sur plateforme en utilisant la solution prototype proposée par l'entrepreneur classé au premier rang (déterminé après l'ECC) afin de confirmer que la solution prototype fonctionnant dans l'espace infonuagique de l'entrepreneur peut être installée et déployée selon l'architecture de solutions et le modèle de services infonuagiques proposé.

   (i) Le test de prototype sur plateforme doit démontrer que le prototype qui s'est démarqué à l'ECC, lorsqu'il est installé et déployé, atteint ou dépasse les résultats de l'ECC de la solution prototype. Le test de prototype sur plateforme sera basé sur les exigences fonctionnelles décrites à l'Appendice A – Évaluation des capacités et de la convivialité (ECC) de l'Énoncé des travaux – Annexe A du contrat.

   (ii) À la demande du Canada, l'entrepreneur doit fournir un soutien et une assistance pour l'installation et le déploiement de sa solution prototype dans l'espace infonuagique protégé B de la GRC.

   (iii) Le Canada a l'intention de mener le test de prototype sur plateforme à la Direction générale de la GRC, dans la région de la capitale nationale, à un emplacement fourni par le gouvernement du Canada qui recrée l'environnement technique décrit à la Section 4.5 – Architecture. Toutefois, le Canada se réserve le droit d'effectuer ce test dans un autre endroit au Canada choisi par l'entrepreneur classé au premier rang, si l'entrepreneur accepte l'entière responsabilité de recréer l'environnement technique décrit à la Section 4.5 – Architecture. Il revient à l'autorité contractante de déterminer si l'entrepreneur a su recréer correctement cet environnement aux fins du contrôle.

b) Si la solution est fournie au moyen de SaaS, le test de prototype sur plateforme permettra de confirmer que le prototype qui s'est démarqué à l'ECC atteint ou dépasse les résultats de la solution prototype à l'ECC, lorsque l'on y accède par l'intermédiaire d'un navigateur Web de la GRC ou un client léger.

c) La solution prototype déployée à des fins de test de prototype sur plateforme doit être une solution prototype fonctionnelle prête pour la production. La solution prototype visée par l'ECC sera utilisée en guise de plus petit produit viable (PPPV). Les caractéristiques et la fonctionnalité décrites à l' l'Appendice C – Modèle de capacité opérationnelle de la SNC seront ajoutées au PPPV pendant la phase 2 du projet. La solution prototype déployée pour le test de prototype sur plateforme ne doit pas nécessiter une mise au point importante avant d'être mise en application.

2.6 Produits livrables de la phase 1

a) Le contractant doit exécuter les produits livrables de la phase 1 de la SNC décrits ci-dessous.

i) **Une réunion de lancement de la phase de prototype** qui doit être prévue au plus tard une (1) semaine après l'attribution du contrat et qui doit :

(1) avoir lieu virtuellement par vidéoconférence, téléconférence ou à un endroit mutuellement convenu dans la région de la capitale nationale du Canada (conformément aux lignes directrices du gouvernement fédéral relatives à la COVID-19);

(2) être présidée par l'autorité contractante de Services publics et Approvisionnement Canada (SPAC);

(3) inclure un ordre du jour de la réunion et une présentation, le cas échéant, à fournir à l'autorité contractante de SPAC au moins deux jours ouvrables avant la réunion de lancement;

(4) Suite à la réunion de lancement de la phase de prototype, l'entrepreneur doit préparer et fournir le procès-verbal de la réunion à l'autorité contractante pour approbation dans un délai de 2 jours ouvrables, avant distribution à toutes les autorités.

ii) **Des séances obligatoires de mobilisation des entrepreneurs**, qui représentent :

(1) Une occasion de collaboration pour le client d'affaires et le responsable technique de la GRC d'interagir avec l'entrepreneur tout au long de la mise au point du prototype afin de répondre aux questions sur le mandat et les exigences du GNCC et fournir une rétroaction sur les prototypes, assurant ainsi une compréhension approfondie des exigences tout en faisant la promotion des utilisateurs au premier plan. Au moins trois séances avec chaque entrepreneur sont prévues. Des séances supplémentaires pourraient être ajoutées au besoin.

iii) **Un plan d'installation de la solution prototype** (si applicable, selon le modèle de services infonuagiques de l'entrepreneur), pour le test de prototype sur plateforme, qui doit inclure, mais sans s'y limiter :

(1) Un ensemble d'instructions (c'est-à-dire un manuel d'installation) qui est clair et suffisamment détaillé pour permettre au Canada de bien comprendre les exigences d'installation de la solution prototype.

(2) Une description technique de la méthode de conditionnement ou de distribution ou des archives d'installation pour chacun des composants d'infrastructure et des composants logiciels utilisés dans la solution prototype.

Remarque : L'installation de la solution prototype sera effectuée par le Programme de GI/TI de la GRC, qui fera appel au fournisseur du prototype pour le soutien et l'assistance techniques, selon les besoins.

iv) **Un plan d'essais d'acceptation de la solution prototype** pour le test de prototype sur plateforme, qui doit inclure :

(1) Une description des procédures de planification, de préparation et de réalisation des essais d'acceptation du prototype sur la plateforme.

Remarque : Les critères d'évaluation de l'acceptation pour le test de prototype sur plateforme seront basés sur les résultats de l'évaluation de la solution de l'entrepreneur et seront fournis par la GRC.

v) **Une solution prototype et la documentation**, devant inclure :

(1) Un accès pour 100 utilisateurs, avec tous les droits d'utilisation de la solution, la documentation sur le logiciel, la garantie, l'hébergement, la maintenance et le soutien (à l'exclusion de la formation), les renonciations, les ententes de non-divulgation ou les autres versions au gouvernement du Canada;

(2) Les documents de référence ou les fichiers d'aide à l'appui de chaque scénario de l'ECC (Récit de l'utilisateur).

vi) **Un plan de gestion de projet pour les travaux de la phase 2 – Ébauche générale**, décrit à la section 6.5 et à la section 7.2, a), iii – Plan de gestion de projet du présent EDT pour plus de détails.

vii) **Un plan de mise en œuvre de la solution pour les travaux de la phase 2 – Ébauche générale**, décrit à la section 7.2, a), vi – Plan de mise en œuvre de la solution du présent EDT pour plus de détails.

Tableau 2-1 : Produits livrables de la phase 1

Nº	Description du produit livrable	Dates de livraison
1	**Réunion de lancement de la phase de prototype**	2 semaines à compter de la date d'attribution du contrat de prototype
2	**Séance de mobilisation des entrepreneurs – Nº 1**	5 semaines à compter de la date d'attribution du contrat de prototype
3	**Séance de mobilisation des entrepreneurs – Nº 2**	10 semaines à compter de la date d'attribution du contrat de prototype
4	**Séance de mobilisation des entrepreneurs – Nº 3**	15 semaines à compter de la date d'attribution du contrat de prototype
5	**Plan d'installation de la solution prototype**, copie numérique remise à l'autorité technique du client et à l'autorité contractante	16 semaines à compter de la date d'attribution du contrat de prototype
6	**Plan d'essais d'acceptation de la solution prototype**, copie numérique remise à l'autorité technique du client et à l'autorité contractante	18 semaines à compter de la date d'attribution du contrat de prototype
7	**Solution prototype et documentation** (dont l'accès pour 100 utilisateurs simultanés), copie numérique remise à l'autorité technique du client et à l'autorité contractante	20 semaines à compter de la date d'attribution du contrat de prototype
8	**Ébauche générale du plan de gestion de projet pour les travaux de phase 2**, copie numérique remise à l'autorité technique du client et à l'autorité contractante	21 semaines à compter de la date d'attribution du contrat de prototype
9	**Ébauche générale du plan de mise en œuvre pour les travaux de phase 2**, copie numérique remise à l'autorité technique du client et à l'autorité contractante	21 semaines à compter de la date d'attribution du contrat de prototype

3. Phase 2 – Solution complète

a) Tous les travaux énumérés aux articles 3 à 7 de la phase 2 – Solution complète sont assujettis et conditionnels à la décision du gouvernement du Canada, et à sa discrétion exclusive, d'exercer l'option irrévocable prévue à l'article 7.1c)i) du contrat visant à autoriser l'entrepreneur à exécuter la totalité ou une partie des travaux décrits dans les présentes.

3.1 Portée des travaux

a) L'entrepreneur doit fournir une solution complète contenant toutes les capacités fonctionnelles et non fonctionnelles décrites à l'Appendice C – Modèle de capacité opérationnelle de la SNC.

b) La solution doit faire preuve d'extensibilité et d'élasticité (en fonction du nombre d'utilisateurs) afin de s'adapter aux fluctuations du volume d'activités et d'opérations.

c) L'architecture de la solution doit être extensible afin de pouvoir accueillir d'éventuelles nouvelles technologies, éléments d'architecture et autres éléments liés à la cybersécurité.

d) La solution peut prendre trois formes : elle peut être gérée par la GRC (h ou PaaS privé dans un espace infonuagique protégé B de la GRC) avec octroi de licences perpétuelles; ou il peut s'agir d'un logiciel-service (SaaS) ou d'une PaaS publique ou d'une combinaison de SaaS et de licences perpétuelles (ci-après « solution hybride »).

e) La solution peut comprendre n'importe quelle combinaison de logiciels commerciaux standards, ainsi que des logiciels sur mesure, ouverts ou API, mais la configuration subséquente doit être conforme aux exigences décrites dans le présent EDT.

f) La solution doit supporter le nombre estimé d'utilisateurs principaux de la solution avec droits d'accès et d'utilisation ainsi que le nombre estimé d'utilisateurs du P3 avec droits d'accès, de téléversement et de consommation d'information tel que fournis à l'Appendice F – Données volumétriques.

g) Les SaaS et les PaaS publiques et privées qui sont proposés comme solutions (y compris les éléments de SaaS/PaaS d'une solution hybride) doivent répondre aux exigences de niveau d'assurance 2 en matière d'assurance (protégé B) de la DAMA-SaaS du gouvernement du Canada ou du Catalogue de services de courtage infonuagique GC (protégé B) de SPC.

h) L'entrepreneur doit installer et déployer la solution selon son modèle de services infonuagiques (modèle à présenter avec la documentation sur l'architecture du système), et la solution doit être compatible avec l'infrastructure réseau du gouvernement du Canada existante et la configuration de sécurité en place.

i) L'entrepreneur doit fournir des services professionnels et de formation sur demande tel que décrites à la Section 6.6 – Ressources du projet et section 3.10 – Formation de l'énoncé des travaux.

3.2 Utilisation de l'intelligence artificielle

a) La solution doit utiliser des méthodes et des techniques d'intelligence artificielle (IA) conformes à la Directive sur la prise de décision automatisée du gouvernement du Canada[1], afin d'en améliorer les résultats et de la rendre plus utile pour les fonctions opérationnelles du GNCC, notamment :

[1] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?_id=32592

i) l'apprentissage machine (AM);

ii) le traitement du langage naturel (TLN);

iii) la reconnaissance des formes;

iv) la reconnaissance d'entités nommées;

v) la reconnaissance de sujets;

vi) l'analyse des sentiments;

vii) la prise de décisions;

viii) le traitement des mégadonnées;

ix) l'analytique en temps réel;

x) l'analytique du texte;

xi) l'analyse du renseignement;

xii) l'analyse des tendances.

b) La solution de l'entrepreneur doit fournir au gouvernement du Canada un degré de transparence acceptable quant aux méthodes et techniques d'IA utilisées. À la demande du gouvernement du Canada, l'entrepreneur doit décrire en détail les constatations de l'IA pour les dossiers du gouvernement du Canada et pour une utilisation potentielle dans les procédures judiciaires. Les processus de prise de décisions automatisés doivent pouvoir être surveillés; on pourra ainsi assurer la transparence et éviter la partialité. L'application des méthodes et des techniques d'IA dans la solution doit soutenir l'obligation de la GRC d'être conforme à la Directive sur la prise de décision automatisée[2] et aux lignes directrices sur l'utilisation responsable de l'intelligence artificielle[3] du gouvernement du Canada (GC).

3.3 Exigences relatives à la gestion de l'information

a) La solution doit prendre en charge les exigences de gestion de l'information (GI) du gouvernement du Canada et y répondre en fournissant, au minimum, les fonctionnalités de GI suivantes :

i) effectuer une recherche en texte intégral sur les métadonnées et les données contenues dans la solution;

ii) restreindre les droits d'accès aux données et renseignements et lever cette restriction sous réserve des exigences législatives. L'accès exigera une autorisation d'accès pour la gestion de l'information;

iii) fournir un journal de vérification de tous les événements pour démontrer l'intégrité des données (p. ex. créations, modifications, suppression, archivage, aliénation [transfert en dehors du contrôle du gouvernement], temps d'arrêt, défaillances du système et accès associés aux renseignements et données;

iv) conserver les données et les renseignements contenus dans la solution pendant une période déterminée en fonction des exigences de conservation des renseignements du GNCC (c.-à-d. au moins 10 années civiles);

---

[2] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592

[3] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai.html

v) purger les renseignements et les données de la solution à la fin de leur période de conservation de la GI associée, y compris les renseignements stockés dans un emplacement archivé dans la solution;

vi) remplacer les dates d'élimination (dates de purge) en cas d'exigence juridique ou opérationnelle dans la solution;

vii) exporter les renseignements et données de la solution dans un format compatible désigné selon le secteur d'activité et la GI;

viii) déterminer les données et les renseignements qui sont divulgués dans le cas d'exigences législatives;

ix) ajouter des champs de métadonnées pour décrire les données conformément à la Norme sur les métadonnées du gouvernement du Canada[4].

3.4 Solution logicielle et documentation

a) L'entrepreneur doit assurer la mise en place complète d'une solution configurée, éprouvée et mise en œuvre et des documents pour une moyenne estimée de 500 utilisateurs simultanés à tous les niveaux à l'échelle nationale et dans les organismes fédéraux d'application de la loi, y compris l'accès à la solution pour environ 2000 utilisateurs ce qui comprend tous les droits d'utilisation de la solution, les documents sur le logiciel, la garantie, la maintenance et le soutien (à l'exception de la formation), les renonciations, les ententes de non-divulgation ou d'autres versions au gouvernement du Canada.

b) Ce produit livrable comprend tous les logiciels et documents liés à tous les aspects de la solution de l'entrepreneur, y compris le système d'exploitation, les documents d'administration du système, les documents sur le guide de l'utilisateur, le code source développé sur mesure et les documents de maintenance du système non précisément désignés comme produit livrable; cependant, il fait partie des documents de la solution globale.

c) Les documents doivent doit être préparés à l'aide d'applications Microsoft Office approuvées par le gouvernement du Canada (Word, Excel, PowerPoint, Visio, Project et Access) et doivent être lisibles et se prêter à la reproduction. Les pages doivent être numérotées de manière séquentielle. En outre, les annexes sont clairement identifiées et font l'objet de renvois dans les documents. Si la solution proposée par l'entrepreneur repose sur un produit commercial, les documents existants doivent être modifiés pour satisfaire à ce produit livrable.

d) Il incombe à l'entrepreneur d'inclure le logiciel et les documents nécessaires pour décrire avec suffisamment de détails les aspects fonctionnels, techniques et de soutien de la solution.

[4] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18909

3.5 Documentation technique de la solution

a) L'entrepreneur doit fournir un document de conception de système (DCS) abordant la conception de la solution livrée. Le DCS de l'entrepreneur doit fournir une seule vue intégrée de l'architecture globale de la solution livrée par l'entrepreneur. Le DCS doit inclure le modèle de services infonuagiques proposé pour la solution. Le DCS doit aussi refléter l'architecture et la configuration définitives, y compris la configuration de sécurité, de la solution.

b) Les documents suivants doivent être fournis au gouvernement du Canada dans le cadre de la solution. Ils peuvent être livrés sous forme de documents individuels ou regroupés dans d'autres produits livrables :

   i) une architecture de système, y compris une architecture de solution complète, le modèle de services infonuagiques et les diagrammes de réseau et de flux de données (voir la Section 4 – Architecture de système pour plus de détails);

   ii) une évaluation et autorisation de sécurité (EAS) qui doit inclure, au minimum, un énoncé de sensibilité (ES), une catégorisation de la sécurité, un concept des opérations de sécurité, un plan d'action et des jalons. La liste complète des produits livrables pour l'EAS sera fournie par la Sous-direction de la sécurité ministérielle (SDSM) de la GRC une fois que la phase de prototype sera terminée et qu'un aperçu de la solution sera disponible;

   iii) un plan de gestion de la sécurité qui décrit :

      (1) les contrôles de sécurité qui doivent être mis en œuvre et surveillés en fonction de l'évaluation de sécurité de l'entrepreneur;

      (2) les rôles et responsabilités de l'entrepreneur en matière de sécurité (pour des détails complets, voir la Section 5 - Plan de sécurité du système Section 5 - Plan de sécurité du système);

      (3) l'emplacement physique de tout membre du personnel chargé de la sécurité, de la configuration ou du soutien;

      (4) le processus pour détecter, signaler et régler les incidents de sécurité;

      (5) le renforcement de la sécurité des systèmes, y compris la gestion continue des correctifs;

   iv) un plan de sauvegarde et de restauration;

   v) un plan de continuité de la technologie de l'information (PCTI) pour atteindre l'objectif de point de reprise (OPR) et l'objectif du délai de rétablissement (ODR);

   vi) un plan de formation des utilisateurs et des administrateurs;

   vii) un plan de gestion de la configuration;

   viii) un plan de sécurité du système comprenant la vérification et la journalisation (Section 4.9 – Journalisation et vérification)

   ix) des documents de formation à l'intention des utilisateurs;

   x) un plan de cycle de vie de l'information, depuis la création initiale des données jusqu'à leur élimination finale.

c) L'entrepreneur doit s'assurer que les documents techniques de la solution sont exacts et mis à jour de façon à refléter la solution.

3.6 Plan de reprise après sinistre

a) L'entrepreneur doit remettre au responsable technique un plan de reprise après sinistre (PRS) pour la solution. Le plan doit inclure un ensemble de politiques, d'outils et de procédures visant à permettre la reprise et la poursuite de l'exploitation de la solution à la suite d'une catastrophe d'origine naturelle ou humaine.

b) L'entrepreneur doit travailler en collaboration avec le gouvernement du Canada pour s'assurer que le PRS relatif à la solution s'intègre efficacement avec le PRS plus large de la GRC pour l'infrastructure technologique de l'entreprise et les systèmes d'applications essentiels qui y sont intégrés.

c) L'entrepreneur doit présenter au Canada un plan d'essais de RS qui documente :

   i) Des procédures d'essais annuels pour confirmer que la RS est correctement mise en œuvre et qu'elle satisfait aux normes applicables, indiquées à la section 3.15 - Disponibilité et rendement de la solution;

   ii) Les résultats attendus et réels des essais de RS;

   iii) Pour chaque écart par rapport au résultat attendu, une description des mesures correctives et un calendrier de mise en œuvre.

d) Le PRS doit décrire de façon suffisamment détaillée comment le gouvernement du Canada peut rapidement se rétablir et reprendre les travaux après qu'un incident majeur imprévu ait eu une incidence sur la solution fournie par l'entrepreneur.

e) L'entrepreneur doit décrire l'approche de rétablissement de la solution et de récupération des données. L'approche de récupération des données doit se référer au plan documenté à la la Section 3.5 – Documentation technique de la solution, la Section 3.5 – Documentation technique de la solution, le plan de sauvegarde et de restauration et le plan de continuité des technologies de l'information.

3.7 Plan d'essais d'acceptation de la solution

a) L'entrepreneur doit préparer un plan d'essais d'acceptation de la solution et de gestion de la qualité qui décrit la façon dont les capacités et les processus fonctionnels et techniques feront l'objet d'essais visant à garantir au gouvernement du Canada que les plans d'essai et de gestion de la qualité de l'entrepreneur sont conformes au modèle de capacités opérationnelles de la SNC et autres exigences définies dans le présent EDT.

b) Le plan d'essais d'acceptation de la solution et le plan de gestion de la qualité doivent être approuvés par le gouvernement du Canada. Les essais d'acceptation de la solution doivent être effectués conformément au plan d'essais d'acceptation et au plan de gestion de la qualité approuvés et selon le plan de mise en œuvre de la solution approuvé.

c) Pendant le développement de la solution, l'entrepreneur doit participer aux activités de gestion de la qualité, y compris les examens avec les ressources du gouvernement du Canada et les utilisateurs de la solution, ainsi que les essais (rendement et régression) de diverses composantes et caractéristiques du système, au besoin, dans le but de garantir l'acceptation.

d) La méthodologie de l'entrepreneur doit suivre des principes et des valeurs permettant d'intégrer fréquemment des étapes de qualité et d'examen tout au long du processus de livraison et d'intégration. Il est prévu que les fonctionnalités de la solution soient développées et déployées au moyen de multiples itérations ou sprints afin de permettre une livraison progressive des fonctionnalités pendant la durée du contrat.

e) La méthodologie de l'entrepreneur doit comprendre des plans d'essai comprenant :

   i) les essais d'acceptation par l'utilisateur;

   ii) les essais de régression;

   iii) les essais avant l'installation;

   iv) les essais de sécurité;

   v) les essais de volume, y compris l'analyse de grands ensembles de données;

   vi) les tests de performance (en fonction des paramètres de rendement fournis à la section 3.18 - Paramètres de rendement);

   vii) les tests de fumée.

f) Le plan d'essais d'acceptation de la solution et le plan de gestion de la qualité doivent décrire l'approche de l'entrepreneur à l'égard des pratiques exemplaires suivantes :

   i) les données des essais pour :

      (1) les essais unitaires (y compris les tests de validation des données et de validation des champs);

      (2) les essais de sprint;

      (3) les essais d'intégration;

      (4) les essais sous contrainte;

      (5) les essais de régression;

      (6) les essais d'acceptation par l'utilisateur;

   ii) les essais et l'acceptation comprenant :

      (1) les essais de sprint;

      (2) la collaboration avec les intervenants;

      (3) la définition de « terminé »;

      (4) les essais unitaires, fonctionnels, de convivialité, d'accessibilité, d'erreur, d'exception, de conformité, d'interopérabilité, d'intégration et de sécurité (y compris les analyses d'évaluation de la vulnérabilité) de bout en bout;

      (5) les essais de reprise après sinistre.

   iii) la version de maintenance et les essais de correctifs, y compris les essais de régression en raison des mises à jour de la solution;

   iv) la description de la façon dont les tests automatisés sont intégrés aux essais de la solution;

   v) la mise à l'essai à chaque sprint et l'inclusion des résultats de l'essai dans la définition « Terminé » de chaque exigence;

vi) pour la qualité, une approche réactive, par des essais, et une approche proactive, par l'encouragement à l'égard de pratiques visant à préparer le terrain pour un travail de qualité. Des exemples d'approches proactives de la qualité comprennent la communication face à face, la programmation par équipes de deux et les normes de codage établies;

vii) la création et l'essai de fonctionnalités plus risquées dans les premiers sprints lorsque les coûts irrécupérables sont encore bas.

g) Le format de ce produit livrable est flexible, et il revient à l'entrepreneur de décider du meilleur format et du nombre d'artefacts (p. ex. diagramme, vues, modèles, catalogues, matrices) qui sont nécessaires. Les artefacts soumis doivent être clairs et concis, bien décrits et permettre au gouvernement du Canada de comprendre comment les exigences ont été satisfaites.

3.8 Rapport d'essai d'acceptation de la solution

a) Le but de ce rapport est de documenter les résultats des essais réalisés pour l'acceptation de la solution avant l'acceptation finale par le gouvernement du Canada.

b) Le rapport d'essai d'acceptation doit consigner les résultats des essais réalisés pour l'acceptation de la solution. Il indique au gouvernement du Canada que la solution a réussi les essais d'acceptation requis et qu'elle respecte les exigences fonctionnelles et techniques énoncées dans le contrat ou qu'elle a échoué les essais d'acceptation, avec les raisons de la défaillance et un plan de mesures correctives prises par l'entrepreneur.

3.9 Déploiement progressif de la solution

a) L'entrepreneur doit, en utilisant une approche itérative, développer continuellement les caractéristiques énumérées dans le carnet de produit qui doivent être classées par ordre de priorité en collaboration avec le client d'affaires de la GRC.

b) L'entrepreneur doit livrer, aux fins d'acceptation, des versions successives de la solution jusqu'à ce que la pleine capacité opérationnelle soit fournie, comme le documente le modèle de capacité opérationnelle.

3.10 Formation

3.10.1 Plan de formation

a) L'entrepreneur doit fournir un plan de formation qui décrit de quelle manière et à quel endroit la formation sera dispensée aux utilisateurs avancés, aux experts en la matière et au personnel de soutien technique.

b) Le plan de formation de l'entrepreneur doit décrire la formation destinée aux utilisateurs avancés et aux experts en la matière suivant un cadre de formation du formateur. La GRC a besoin d'une formation des utilisateurs et des instructeurs, de sorte que les instructeurs potentiels, les utilisateurs avancés et les experts en la matière puissent donner à leurs collègues une formation sur l'utilisation de la solution.

c) Le plan de formation de l'entrepreneur doit décrire la formation des ressources techniques applicable pour le personnel de soutien technique.

d) Le plan de formation doit décrire de quelle manière la formation sera dispensée à de petits groupes d'utilisateurs (utilisateurs avancés, experts en la matière, utilisateurs finaux ou ressources techniques) selon les besoins.

e) Le plan de formation de l'entrepreneur doit décrire de quelle façon il prévoit fournir des ressources de formation initiales et mises à jour bilingues (en français et en anglais), notamment :

   i) une aide en ligne;

   ii) une formation en ligne;

   iii) des documents en anglais et en français;

   iv) du matériel de formation mis à jour au fil du temps pour couvrir les nouvelles fonctionnalités ajoutées;

   v) une description du matériel de formation à fournir.

3.10.2 Matériel de formation

a) L'entrepreneur doit fournir des copies électroniques en anglais et en français des manuels d'utilisation, des manuels techniques et de tout autre document à l'intention de l'utilisateur requis pour lui permettre d'apprendre, d'utiliser et de tenir à jour la solution.

b) Les manuels de fonctionnement, les manuels techniques et les autres documents pour l'utilisateur fournis par l'entrepreneur au Canada et devant être utilisés avec la solution doivent décrire le fonctionnement de la solution suffisamment en détail pour permettre à des employés du Canada d'utiliser toutes les fonctions et caractéristiques de la solution sans l'aide de l'entrepreneur.

c) L'entrepreneur doit fournir des manuels d'utilisation et du matériel de formation bilingues (anglais et français) à l'aide des applications Microsoft Office approuvées par le gouvernement du Canada (Word, Excel, PowerPoint, Visio, Project et Access).

d) Les données et les documents utilisés aux fins de formation ne doivent contenir aucun renseignement PROTÉGÉ. Les données sur la cybercriminalité dans l'environnement de formation doivent être fictives sans ressemblance avec des personnes ou des données non fictives.

3.10.3 Prestation de la formation

a) L'entrepreneur doit fournir une formation sur la solution à quarante (40) utilisateurs avancés et experts en la matière suivant un cadre de formation du formateur.

b) L'entrepreneur doit fournir une formation technique relative à la solution à vingt-cinq (25) ressources de soutien technique responsables de la maintenance et du soutien continus de la solution.

c) L'entrepreneur peut être appelé à dispenser une formation sur la solution à de petits groupes d'utilisateurs (utilisateurs avancés, experts en la matière ou ressources techniques) selon les besoins.

d) Toutes les exigences relatives à la formation qui vont au-delà de la formation initiale des utilisateurs avancés, des experts en la matière et des ressources techniques seront remplies au moyen d'autorisations de tâches individuelles.

3.11 Évaluation des facteurs relatifs à la vie privée

a) L'entrepreneur doit travailler en collaboration avec le gouvernement du Canada afin de fournir un document d'évaluation des facteurs relatifs à la vie privée (EFVP) qui doit, au minimum, inclure les renseignements suivants :

   i) une liste de toutes les mesures prises par l'entrepreneur afin de protéger les renseignements personnels et les dossiers, conformément aux obligations réglementaires;

   ii) les procédés administratifs, flux de données et procédures de collecte, de transmission, de traitement, de stockage, d'élimination et de consultation des renseignements, y compris des renseignements personnels;

   iii) les autres exigences relatives à la sécurité et à la protection des renseignements personnels et les recommandations de l'entrepreneur qui doivent être examinées par le gouvernement du Canada.

b) L'entrepreneur doit aborder expressément les éléments de l'EFVP suivants en détail :

   i) les stratégies de protection des renseignements personnels de la solution, y compris la description du traitement des renseignements tout au long de leur cycle de vie;

   ii) les méthodes qui seront employées pour la collecte, l'utilisation, la conservation, la divulgation et l'élimination des renseignements personnels uniquement aux fins des travaux précisés dans la solution;

   iii) les méthodes qui seront employées pour restreindre l'accès aux renseignements personnels et aux dossiers aux personnes autorisées seulement (en fonction du besoin de savoir) et exclusivement aux fins d'exécution des travaux prévus dans la solution;

   iv) un protocole privilégié en cas d'atteinte à la protection des renseignements personnels;

   v) les méthodes que l'entrepreneur entend employer pour veiller à ce que les exigences en matière de protection des renseignements personnels du Canada décrites dans la *Loi sur la protection des renseignements personnels*[5], la *Loi sur l'accès à l'information*[6] et la *Loi sur la Bibliothèque et les Archives du Canada*[7] soient respectées tout au long de l'exécution des travaux et pendant toute la durée du contrat;

   vi) toute nouvelle mesure que l'entrepreneur entend mettre en œuvre pour protéger les renseignements personnels et les dossiers en fonction de leur classification de sécurité;

   vii) les mesures que l'entrepreneur entend prendre pour que les rapports renfermant des renseignements personnels soient stockés ou transmis de façon sûre, en fonction de leur classification de sécurité;

   viii) la description de la façon dont l'entrepreneur entend s'assurer que son personnel est formé à la protection des renseignements personnels et aux principes connexes.

---

[5] https://laws-lois.justice.gc.ca/fra/Lois/P-21/index.html

[6] https://laws-lois.justice.gc.ca/fra/lois/a-1/

[7] https://laws-lois.justice.gc.ca/fra/lois/L-7.7/index.html

c) L'entrepreneur doit fournir une explication détaillée des menaces réelles et potentielles touchant les renseignements personnels ou les dossiers, accompagnée d'une évaluation des risques liés à ces menaces et exposant la pertinence des mesures existantes visant à prévenir ces risques.

d) L'entrepreneur doit démontrer que les données et renseignements confidentiels et exclusifs du gouvernement du Canada seront protégés adéquatement.

e) L'entrepreneur doit démontrer comment il établira un équilibre efficace entre la nécessité d'effectuer des essais de haute qualité et la protection de l'information des utilisateurs.

3.12 Plan de transition

a) L'entrepreneur doit fournir un plan de transition qui décrit comment la solution sera menée jusqu'à un statut opérationnel complet et intégrée à l'architecture cible (voir la Section Section 4.5 – Architecture) et aux opérations de programmes d'activités de la GRC.

b) Le plan de transition doit contenir une brève description des principales tâches relatives au processus de transfert, des ressources requises pour soutenir le fonctionnement de la solution et de toutes les exigences de maintenance continue propres au site.

c) Pendant la période de transition, l'entrepreneur doit mener des activités pour assurer une transition efficace et complète de la solution, sans interruption de la prestation des services au gouvernement du Canada.

d) Le plan de transition du projet doit comprendre au moins les éléments énumérés ci-dessous :

   i) les activités et les documents requis pour terminer le transfert final et le transfert de connaissances de l'entrepreneur aux ressources du gouvernement du Canada pour le fonctionnement du cycle de vie et la maintenance;

   ii) les principaux jalons correspondant aux principaux points de vérification du calendrier de transition qui permettent de mesurer l'avancement du projet;

   iii) le calendrier de transition;

   iv) les responsabilités et les tâches et préciser qui est responsable de chacune des activités et qui les exécutera;

   v) les hypothèses de planification qui sont formulées lors de l'élaboration du plan de transition;

   vi) les risques relatifs à la transition, y compris la catégorie du risque et les mesures d'atténuation.

e) L'entrepreneur doit assumer toutes les obligations contenues dans le plan de transition conformément au calendrier de transition.

f) Pendant la période de transition, l'entrepreneur doit assurer le transfert des connaissances au gouvernement du Canada, comme il est décrit dans le plan de transition.

g) L'entrepreneur doit répondre aux questions concernant les activités de transition et tous les travaux en cours pour assurer une transition harmonieuse et la prestation ininterrompue des services au gouvernement du Canada.

h) L'entrepreneur livrera le plan de transition et les mises à jour conformément au calendrier décrit dans la liste des produits livrables de la phase 2 dans les présentes.

3.13 Plan de transition de sortie

a) L'entrepreneur doit fournir un plan de transition de sortie (applicable aux SaaS et aux PaaS publiques) décrivant les activités et les processus à mettre en place si la PaaS publique ou le SaaS prévu dans l'entente est abandonné (p. ex. faillite du fournisseur du SaaS ou de la PaaS).

b) Le plan de transition de sortie doit prévoir :

   i) le retour des données et des dossiers au Canada dans le format du fournisseur et un format adapté à la plateforme;

   ii) l'élimination sûre et permanente des ressources et des actifs informationnels (p. ex. matériel, entrepôt de données, dossiers, mémoire) de l'environnement du fournisseur;

   iii) l'élimination sûre et permanente des actifs informationnels créés par reproduction pour assurer une haute disponibilité, la sauvegarde des données et la reprise après sinistre;

   iv) le soutien de l'entrepreneur dans le cadre de toutes les activités associées à la transition d'un SaaS ou d'une PaaS publique à une autre solution;

   v) la continuité des activités.

c) À la demande du Canada, l'entrepreneur doit prouver au moyen de pièces justificatives qu'il a bel et bien effacé, purgé ou détruit de manière permanente toutes les ressources associées à l'utilisation du SaaS ou de la PaaS publique par le Canada.

d) Pour ce qui est des services de migration et de transition, l'entrepreneur accepte que, jusqu'à la fin du contrat, si le Canada demande des services de migration ou de transition, il l'aide avec diligence à faire la transition du contrat au nouveau contrat avec un autre fournisseur ou à assurer la migration des données du client vers l'environnement d'un nouveau fournisseur, sans frais supplémentaires pour ces services, outre ceux énoncés dans la Base de paiement.

3.14 Maintenance et soutien de la solution

3.14.1 Période de garantie du logiciel

a) Dans le présent EDT, sauf mention contraire dans le contrat, la « période de garantie du logiciel » désigne une période de douze (12) mois à partir de la date à laquelle le logiciel sous licence est accepté conformément aux conditions du contrat, à l'exception des travaux prévus dans le cadre de la garantie et des autres travaux éventuels prévus en vertu du contrat et qui devraient avoir lieu après le début de la période de garantie du logiciel.

3.14.2 Évolution DE LA SOLUTION

a) Dans un environnement où la technologie évolue rapidement et où les pratiques de cybercriminalité changent, l'entrepreneur doit démontrer des plans et des feuilles de route des produits continus, formuler des conseils et informer la GRC des nouvelles tendances pour garantir que la solution reste alignée sur les pratiques exemplaires de l'industrie, de même que sur les avancées technologiques et analytiques tout au long du contrat et jusqu'à la fin de la période de garantie.

b) La solution de l'entrepreneur doit permettre la personnalisation de la couche de présentation, permettant à la GRC d'élaborer de nouveaux flux de travail, processus d'approbation, définitions de rôle, droits d'accès, modèles, rapports et écrans, afin de fournir des fonctionnalités supplémentaires non prévues dans la solution initiale.

c) L'entrepreneur doit fournir un moyen de collaborer avec la GRC pour le développement de nouvelles mises à jour de fonctionnalités ainsi que des correctifs de maintenance, pendant le développement et après la livraison de la capacité opérationnelle complète.

3.14.3 Soutien et maintenance

a) Jusqu'à la fin de la période de garantie, l'entrepreneur doit :

i) Suivre les incidents et les cas grâce au système de gestion des billets de la GRC. Des rapports hebdomadaires et mensuels sur les incidents (billets) et leur règlement sont requis et doivent être remis au responsable technique; certains incidents peuvent nécessiter la présence de l'entrepreneur sur place dans la région de la capitale nationale du Canada.

ii) Tenir des réunions mensuelles pour discuter des incidents majeurs liés à la solution et transmettre les connaissances sur les solutions et initiatives de développement en cours. Le billet doit décrire le problème et les incidents en détail, s'assurer que les examens ont été effectués, que les mesures correctives ont été approuvées et que les activités d'assurance de la qualité (AQ) après l'incident ont été menées à bien.

iii) Veiller à ce que son personnel soit qualifié et capable de répondre aux questions des clients et des utilisateurs et, dans la mesure du possible, de résoudre les problèmes des utilisateurs par téléphone ou par courriel et de fournir des conseils sur les fonctionnalités, la configuration et les questions techniques.

iv) Doit aviser le gouvernement du Canada des changements à venir et des problèmes opérationnels potentiels liés aux nouvelles versions de la solution et envoyer des notifications aux utilisateurs concernant tout changement qui pourrait avoir une incidence sur le service.

v) Fournir une procédure documentée de la priorité des incidents qui doit comprendre les définitions de la gravité des problèmes (p. ex. critique, majeur et mineur) et les délais d'intervention et de résolution correspondants.

vi) Désigner un représentant des comptes qui agira à titre de point de contact hiérarchique pour le soutien et les problèmes liés aux comptes.

vii) Fournir un soutien de niveau 3 pour la solution complète ainsi que le développement, la mise en œuvre, la configuration et le soutien de nouvelles fonctionnalités. On s'attend à ce que le gouvernement du Canada ait des responsabilités de soutien à l'égard du service (c.-à-d. soutien de premier niveau et gestion du renouvellement de l'ensemble des logiciels et licences de locataire). Voir l'annexe D – Définitions et interprétations pour les définitions des niveaux de soutien.

viii) Inclure les capacités de soutien, y compris la formation sur les fonctionnalités et les améliorations.

3.14.4 Gestion des événements et des incidents

a) L'entrepreneur doit résoudre les incidents en collaboration avec le gouvernement du Canada et toute autre tierce partie à la demande du gouvernement du Canada, de la façon suivante :

i) l'entrepreneur doit fournir au gouvernement du Canada des mises à jour sur l'état des incidents, selon des niveaux de priorité et à une fréquence précisés par le gouvernement du Canada. Les mises à jour sur l'état doivent être fournies par courriel et, lorsque le gouvernement du Canada le demande, verbalement;

ii) l'entrepreneur doit fournir une estimation du temps de résolution à chaque mise à jour, dans le billet d'incident et, lorsque le gouvernement du Canada le demande, verbalement;

iii) l'entrepreneur doit s'assurer que l'état d'avancement et les mises à jour, la cause fondamentale et la résolution présentent des descriptions claires en utilisant des mots complets, des phrases et une grammaire appropriée en anglais ou en français;

iv) lors de la création ou de la mise à jour d'un billet d'incident, l'entrepreneur doit utiliser le système de gestion des billets de la GRC;

v) l'entrepreneur doit documenter, dans le registre des activités des billets d'incidents, l'ensemble des éléments suivants :

(1) le signalement d'incidents par la direction ou à la suite d'un problème technique;

(2) les interactions avec les tiers;

(3) les détails relatifs à l'enquête, au dépannage et à l'analyse, les activités et les communications de résolution concernant les incidents figurant dans le registre des activités des billets d'incidents.

vi) l'entrepreneur doit consigner dans le billet d'incident toute directive que le gouvernement du Canada fournit en fonction de la fréquence des mises à jour, du changement de priorité et de l'acheminement aux échelons supérieurs, et inclure le nom du représentant de la GRC qui fournit chaque directive;

vii) l'entrepreneur doit déterminer et documenter les facteurs de cause (c.-à-d. les causes fondamentales) de tous les incidents lorsqu'ils sont connus;

viii) l'entrepreneur doit élaborer des solutions de contournement pour gérer les incidents dans la mesure du possible, jusqu'à ce que la cause fondamentale de l'incident ait été gérée (ou lorsque les causes fondamentales sont inconnues).

ix) L'entrepreneur doit fournir un document d'information par rapport à un incident dans un délai d'un jour ouvrable suivant une demande du gouvernement du Canada concernant un incident. Le document doit être présenté selon un format précisé par le gouvernement du Canada.

x) L'entrepreneur doit travailler avec le Canada pour élaborer et mettre en œuvre des rapports postérieurs à un incident et des plans de mesures préventives. L'entrepreneur doit informer le gouvernement du Canada au préalable s'il constate qu'il ne respectera pas les dates cibles précisées dans ses plans d'action.

xi) L'entrepreneur doit fournir au gouvernement du Canada une description claire de chacun des outils, systèmes et applications qu'il utilise ou qui sont mis à la disposition du gouvernement du Canada.

3.15 Disponibilité et rendement de la solution

a) La solution doit être disponible vingt-quatre (24) heures par jour et trois cent soixante-cinq (365) jours par année avec un temps en service moyen de 99,45 % sur un mois.

b) Aux fins de la planification de la continuité des activités pour la SNC :

i) Le temps d'arrêt maximum autorisé pour le SNC est de 4 heures;

ii) L'objectif de temps de reprise est de 1 jour;

iii) L'objectif de point de reprise est de 4 jours.

c) Aux fins de la planification de la continuité des activités, les niveaux de service minimums que le Canada cherchera à soutenir pendant une période de reprise sont, en référence à l'Appendice C – Modèle de capacité opérationnelle de la SNC :

i) 3.0 SNC – Capacités du portail des partenaires policiers (P3), et

ii) 4.0 SNC – Capacités de services fonctionnels, soutenues par un sous-ensemble de,

iii) 5.0 SNC – GCO – Capacités techniques/de la solution.

Les capacités définies en 1.0 SNC – Capacités de signalement public incombent à la GRC et les capacités définies en 2.0 SNC – Capacités de gestion des cas sont soumises à un objectif de reprise du niveau de service moins prioritaire.

d) La solution doit être en mesure de prendre en charge, au minimum, les volumes détaillés à l'Appendice F – Données volumétriques dans les présentes, sans diminution du rendement.

e) Le Canada a la responsabilité de soutenir la disponibilité et le rendement du site Web de signalement destiné au public.

3.16 Utilisateurs

a) La solution doit pouvoir prendre en charge jusqu'à cinq cents (500) utilisateurs simultanés tout en traitant les volumes énoncés à l'Appendice F – Données volumétriques ci-dessous, sans dégradation de la performance.

b) L'Appendice F – Données volumétriques fournit un nombre total approximatif d'utilisateurs principaux (personnel interne du GNCC et de la GRC) qui auront des droits d'accès et d'utilisation de la solution, ainsi que d'utilisateurs du P3 qui téléverseront et consommeront de l'information recueillie par la solution par le truchement du portail.

3.17 Volumes de la solution

a) Voir l'Appendice F – Données volumétriques pour connaître les chiffres estimatifs de croissance de volume associés à l'utilisation de la solution sur huit (8) ans.

b) Le volume des transactions de l'Appendice F – Données volumétriques décrivent uniquement les entrées. Les transactions internes, les notifications, le flux de travail et les requêtes automatiques ne sont pas inclus dans les volumes. Les transactions internes dépendront de la solution de l'entrepreneur.

c) Ces données sont fournies à titre informatif et ne confirment aucunement que l'usage futur du Canada y correspondra.

d) La solution de l'entrepreneur doit être assez élastique et extensible pour s'adapter à des volumes d'utilisateurs, d'opération et de données plus ou moins élevés, ainsi qu'à de courtes fluctuations au chapitre de l'acquisition de données et des modèles de traitement.

3.18 Paramètres de rendement

Compte tenu des volumes estimés et des exigences en matière de soutien technique, la solution doit satisfaire aux exigences en matière de rendement ci-dessous :

Tableau 3-1 : Temps de réponse maximal pour la SNC

Composant	Activités normatives	Temps de réponse maximal (secondes)
Interface utilisateur de la SNC	• Ouvrir une session • Ouvrir une page de saisie/de modification de données • Enregistrer une transaction • Transmettre ou assigner une tâche	1
	• Interroger le dépôt de données de la SNC (afficher les résultats de la recherche)	Moy. 2 sec. – max. 5 sec.
	• Ouvrir une file d'attente • Ouvrir un tableau de bord	2
Interface utilisateur du P3	• Ouvrir une session • Ouvrir une page de saisie de données	1

Composant	Activités normatives	Temps de réponse maximal (secondes)
	• Enregistrer une transaction	
	• Interroger le dépôt de données de la SNC (afficher les résultats de la recherche)	Moy. 2 sec – max. 5 sec
	• Ouvrir un tableau de bord • Ouvrir une file d'attente	Moy. 2 sec. – max. 3 sec.
Indexation/analyse syntaxique	• Extraction de données automatisée • Ingestion de données structurées et non structurées (courriel, demande P3)	Quasi temps réel
Corrélation	• Comparaison des données extraites à celles du dépôt de données de la SNC • Comparaison des nouveaux dépôts aux données existantes	Quasi temps réel

3.19 Loi sur les langues officielles[8]

a) La solution doit être conforme à la *Loi sur les langues officielles*, y compris au minimum les éléments suivants :

i) La qualité et le niveau de langue de la solution et des messages, instructions, logiciels et documents qui y sont associés doivent être équivalents en anglais et en français.

ii) Les messages d'erreur de la solution doivent apparaître dans la langue de préférence de l'utilisateur ou être bilingues et doivent être équivalents en anglais et en français.

iii) Les instructions et directives relatives à la solution doivent apparaître dans la langue de préférence de l'utilisateur.

iv) Les titres de la solution, dans leur intégralité, doivent avoir la même signification dans les deux langues officielles.

v) Le texte alternatif au chapitre de l'accessibilité est produit dans la langue choisie par l'utilisateur de la solution.

vi) Les légendes et les textes des images et des graphiques de la solution doivent être produits de façon équivalente en anglais et en français.

vii) Les rapports doivent être produits dans la langue demandée par l'utilisateur ou sont bilingues (anglais et français).

viii) Quand un utilisateur choisit de changer sa langue de préférence, dans les paramètres de la solution, ce changement doit s'appliquer immédiatement, sans que l'utilisateur doive sortir de l'interface.

[8] https://laws-lois.justice.gc.ca/fra/lois/o-3.01/

ix) Utilisation d'icônes universelles (normalisées) pour les différents menus et outils de la solution (si possible), au lieu d'éléments EN ou FR en toutes lettres, avec affichage au survol par la souris et texte alternatif dans la langue choisie par l'utilisateur.

x) Une recherche effectuée dans l'interface graphique de la solution doit donner les mêmes résultats en anglais et en français. Si les mêmes critères de recherche sont saisis dans une interface utilisateur en français et une interface utilisateur en anglais, le résultat doit être le même.

xi) La documentation d'aide doit être fournie en anglais et en français.

xii) Les instructions et les directives de la page d'aide doivent être fournies dans les deux langues officielles du Canada.

xiii) Le Centre d'appel de l'entrepreneur doit fournir des services équivalents dans les deux langues officielles du Canada.

3.20 Règles pour l'accessibilité des contenus Web (WCAG)

a) La solution doit être conforme aux WCAG 2.0[9] et à la norme sur l'accessibilité du Web[10] du gouvernement du Canada, comme suit :

i) La solution doit être accessible à l'aide de technologies d'assistance et de divers navigateurs Web, tels qu'Internet Explorer, Firefox, Chrome, Safari et Edge.

ii) L'information, la structure et les relations véhiculées par la présentation doivent être déterminées par un programme informatique ou sont disponibles sous forme de texte.

iii) Lorsque l'ordre de présentation du contenu a un effet sur sa signification, un ordre de lecture correct doit être déterminé par programme informatique.

iv) Toutes les fonctions du contenu doivent être contrôlées par une interface clavier qui n'exige pas de rythmes de frappe particuliers, sauf lorsque la fonction sous-jacente nécessite des données indiquant la trajectoire donnée par l'utilisateur en plus des points finaux.

v) Si la cible de saisie du clavier peut être positionnée sur un élément de la page à l'aide d'une interface clavier, réciproquement, elle peut être déplacée hors de cette même composante simplement à l'aide d'une interface clavier et, si ce déplacement exige plus que l'utilisation d'une simple touche flèche ou tabulation ou toute autre méthode standard de sortie, l'utilisateur est informé de la méthode permettant de déplacer la cible de saisie hors de cette composante.

vi) Un mécanisme doit permettre de contourner les blocs de contenu reproduits dans plusieurs pages Web.

vii) Quand une composante de l'interface utilisateur reçoit la cible de saisie, il ne doit pas amorcer un changement de contexte.

viii) Le changement de paramètre d'une composante d'interface utilisateur ne doit pas entraîner de changement de contexte, à moins que l'utilisateur n'ait été avisé de ce comportement avant d'utiliser la composante.

---

[9] https://www.w3.org/TR/WCAG20/

[10] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601

ix) À moins que les spécifications ne le permettent, dans un contenu mis en œuvre au moyen d'un langage de balisage, les éléments ont des balises de début et de fin complètes, ils sont imbriqués conformément à leurs spécifications, ils ne doivent pas contenir d'attributs dupliqués, et chaque ID doit être unique.

x) Pour toute composante d'interface utilisateur (comprenant, mais sans y être limité, des éléments de formulaire, liens et composantes générés par des scripts), le nom et le rôle doivent être déterminés par un programme informatique; les états, les propriétés et les valeurs qui peuvent être paramétrés par l'utilisateur doivent être définis par programmation, et la notification des changements de ces éléments doit être accessible aux agents utilisateurs, y compris les technologies d'assistance.

xi) Le contenu ne doit pas limiter son affichage et son fonctionnement à une seule orientation d'affichage, comme le portrait ou le paysage, à moins qu'une orientation d'affichage spécifique soit essentielle.

xii) Dans un ensemble de pages Web, les mécanismes de navigation qui se répètent sur plusieurs pages Web doivent se présenter dans le même ordre relatif chaque fois qu'ils sont répétés, à moins qu'un changement soit amorcé par l'utilisateur.

xiii) Dans un ensemble de pages Web, les composantes qui ont la même fonction doivent être identifiées de la même façon.

xiv) Toute interface utilisateur utilisable au clavier doit avoir un mode de fonctionnement dans lequel l'indicateur de mise au point du clavier est visible.

4. Architecture de système

a) L'entrepreneur doit fournir une architecture décrivant l'organisation fondamentale de la solution au gouvernement du Canada. L'architecture doit inclure le modèle de services infonuagiques, les composantes faisant partie de la solution, les relations entre les composantes et l'environnement, la connectivité au réseau dans l'architecture ainsi que les flux de données et les principes guidant la conception, le développement et le déploiement de la solution.

b) Le format de livraison de l'architecture est flexible, et il revient à l'entrepreneur de décider du meilleur format et du nombre d'artefacts (par exemple, diagramme, vues, modèles, catalogues, matrices) qui sont requis. Les artefacts soumis doivent être clairs et concis, bien décrits et permettre au Canada de comprendre non seulement la solution, mais également la façon dont les exigences sont respectées.

4.1 Exigences générales

a) Les points suivants fournissent des conseils généraux à l'entrepreneur et ne doivent pas être considérés comme une liste exhaustive des exigences ou des produits livrables :

i) L'entrepreneur doit expliquer comment l'architecture proposée se conformera à l'architecture cible (Section 4.5 – Architecture cible) et, lorsque la solution de l'entrepreneur diffère, l'entrepreneur doit décrire comment l'architecture proposée remplace ou améliore l'architecture cible;

ii) L'entrepreneur doit décrire l'architecture technique qui comprend les composantes technologiques habilitantes et tout produit ou service tiers requis pour prendre en charge la mise en œuvre, la configuration et le fonctionnement de la solution proposée;

iii) L'entrepreneur doit décrire l'architecture de réseau qui comprend tout point d'intégration supposé à l'infrastructure du gouvernement du Canada et à l'espace infonuagique Protégé B de la GRC;

iv) L'entrepreneur doit décrire l'architecture de l'information qui inclut tout flux de l'information et les liens de dépendance pour la migration, la sauvegarde et la récupération de données;

v) L'entrepreneur doit décrire l'architecture de sécurité qui répond à tous les problèmes de sécurité indiqués dans les présentes, à la Section 4.8 – Gestion de l'identité et de l'accès.

vi) L'entrepreneur doit décrire le modèle de services infonuagiques proposé et fournir des détails sur :

(1) l'ensemble des services et des ressources infonuagiques qui seront hébergées dans l'espace infonuagique protégé B de la GRC (IaaS et PaaS privée);

(2) toutes les ressources infonuagiques que la GRC devra fournir pour soutenir les services et les ressources susmentionnés (p. ex. ordinateurs, entrepôt de données, réseau, file d'attente de messages);

a) inclure des attributs de ressource précis (région, unités centrales, mémoire, nbre d'instances, sur demande/réservé, etc.) et inclure les numéros de pièces du fournisseur de services infonuagiques, UGS, etc. afin que l'autorité technique puisse établir avec exactitude le coût des ressources infonuagiques à fournir à la GRC;

(3) l'ensemble des services et des ressources infonuagiques hébergés par le fournisseur de services infonuagiques de l'entrepreneur (SaaS ou PaaS publique) et leur niveau de conformité avec la DAMA-SaaS et le catalogue des services de courtage infonuagique GC (protégé B) de SPC;

(4) l'intégration des services et des ressources infonuagiques proposés à l'architecture des solutions.

vii) Le modèle de services infonuagiques de l'entrepreneur doit tenir compte des éléments suivants :

(1) trois environnements distincts : (1) mise au point; (2) mise à l'essai; et (3) production, avec une capacité d'autoévaluation, au besoin;

(2) la capacité d'élasticité et d'extensibilité pour pouvoir s'adapter aux nouveaux besoins en matière d'environnement, ainsi qu'aux fluctuations du volume d'opérations et à ses pics imprévus;

(3) les exigences en matière de continuité des activités et de haute disponibilité (voir la section 3.15 - Disponibilité et rendement de la solution);

(4) l'optimisation des coûts, l'efficacité opérationnelle et la surveillance;

(5) la capacité de respecter les paramètres de rendement indiqués (voir la section 3.18 - Paramètres de rendement);

(6) la capacité de s'adapter à la croissance continue des volumes d'utilisateurs et de solutions, année après année (voir l'Appendice F – Données volumétriques).

viii) L'entrepreneur doit fournir de l'information claire dans le tableau 1 de l'Appendice G – Tableaux de référence pour le modèle de services infonuagiques afin que l'autorité technique puisse déterminer l'ensemble des ressources infonuagiques que la GRC doit fournir pour sa solution afin de pouvoir l'utiliser et obtenir le soutien nécessaire.

b) L'architecture de la solution proposée doit démontrer comment elle se conformera aux normes numériques du Gouvernement du Canada[11].

c) L'architecture de la solution proposée doit démontrer comment elle se conformera aux normes d'architecture d'entreprise du gouvernement du Canada[12].

d) L'entrepreneur devrait tirer parti des produits commerciaux ou des composantes ouvertes pour offrir des fonctionnalités lorsque cela est possible, par opposition aux solutions exclusives développées sur mesure.

e) L'entrepreneur doit fournir une feuille de route de l'architecture pour décrire les composantes et les caractéristiques qu'il fournira et un calendrier des dates auxquelles ces composantes seront incluses dans l'architecture.

---

[11] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/normes-numeriques-gouvernement-canada.html

[12] https://wiki.gccollab.ca/Government_of_Canada_Architectural_Standards_[en anglais seulement]

4.2 Intégration avec l'environnement de la GRC

4.2.1 Fonds de renseignements de la GRC obligatoires

a) La solution de l'entrepreneur doit utiliser les fonds de renseignements de la GRC conformes aux normes d'entreprise pour remettre les parties de la solution énumérées dans le Tableau 4 1 : Composantes obligatoires de la GRC. Les licences utilisées pour ces composantes ne doivent pas être incluses dans l'établissement des coûts de la solution pour le gouvernement du Canada.

Tableau 4-1 :Composantes obligatoires de la GRC

Composant	Description
Azure Active Directory	Norme de gestion de l'identité et de l'accès de la GRC
Environmental Systems Research Institute (Esri)	Outil normalisé de la GRC pour le SIG et l'analyse cartographique

4.3 Interopérabilité

a) La solution doit être configurée pour permettre l'interopérabilité avec les applications existantes :

i) la solution doit fournir une architecture extensible;

ii) la solution doit permettre d'extraire toutes les données opérationnelles et de les transférer vers un entrepôt de données externe au moyen d'interfaces en vrac;

iii) l'extraction de données par fichiers doit prendre en charge une vaste gamme de formats de fichiers;

iv) la solution doit fournir la capacité d'exporter et d'importer des données par l'entremise d'une fonction qui facilite l'extraction, la transformation et le chargement, prête à l'emploi ou d'autres plateformes commerciales (p. ex. DataStage, [IBM] ou d'autres logiciels libres);

v) la solution doit fournir la capacité d'importer et d'exporter des données de référence et opérationnelles reçues en vrac (p. ex. en provenance d'organismes d'application de la loi ou d'utilisateurs, les données existantes du Centre antifraude du Canada [CAFC]) vers ou depuis le dépôt de données de la SNC au moyen d'une interface de programmation d'applications (API) et d'une interface en vrac;

vi) la solution doit permettre l'intégration avec les systèmes existants du CAFC et les données associées;

vii) la solution doit fournir la capacité d'utiliser les API de services Web synchrones externes conformément aux normes de l'industrie ouverte lorsque la source autorisée de ces données ou fonctionnalités provient d'autres systèmes;

viii) la solution doit fournir la capacité de prendre en charge le protocole TLS 1.2 (protocole de sécurité de la couche transport) pour toutes les interfaces à un niveau minimal de sécurité de la connectivité;

ix) la solution doit fournir la capacité permettant que les interfaces gèrent efficacement les cas où les systèmes externes font l'objet de défaillances ou ne sont pas disponibles;

x) la solution doit protéger les renseignements grâce à des méthodes d'authentification sécurisées utilisant des normes ouvertes (y compris, mais sans s'y limiter, OpenID, OAuth ou SAML);

xi) toutes les API doivent être exposées au moyen de liaisons et de protocoles normalisés ouverts, y compris mais sans s'y limiter : transfert d'état représentationnel (REST) à l'aide de JavaScript Object Notation (JSON) ou de langage de balisage extensible (XML) selon les besoins du système d'interface;

xii) toutes les API doivent permettre de donner accès à des données sous la forme d'entités opérationnelles ou de schémas d'objet non exclusifs. Plus précisément, les API doivent pouvoir résumer les tableaux ou les structures de données brutes principaux;

xiii) les API doivent respecter les normes du gouvernement du Canada sur les API[13];

xiv) la solution doit avoir la capacité de prendre en charge l'intégration de données provenant de sources externes et la génération de rapports sur plusieurs domaines d'information à l'aide de REST avec JSON et XML.

4.4 Site Web de signalement destiné au public

a) Contexte

i) Le site Web de signalement destiné au public que la GRC a créé est un site Web convivial que les victimes et les petites et moyennes entreprises touchées pourront utiliser pour signaler un large éventail d'incidents de cybercriminalité, y compris les cybercrimes proprement dits (p. ex. logiciels malveillants, piratage) et ceux motivés par l'appât du gain (p. ex. cyberfraude, vol d'identité, contrefaçon, extorsion), outre la fraude traditionnelle

ii) Les signalements publics seront intégrés par la solution, qui fournira par la suite les diverses composantes d'analyse, de coordination et d'harmonisation pour ajouter de la valeur grâce à l'enrichissement des données. En utilisant le P3, la solution aura la possibilité de communiquer le signalement aux services de police compétents (SPC) en fonction de la géolocalisation de la victime. Les signalements reçus par l'entremise de l'application Web de signalement de cybercriminalité seront stockés dans le référentiel de la solution fourni par l'entrepreneur.

iii) Les signalements publics comprendront, au minimum (le cas échéant), les types d'entités de données et les exigences d'interface suivants :

(1) Information sur le consentement : Consentement pour la collecte et la communication de renseignements;

(2) Information sur la plainte : un plaignant, y compris les renseignements de base et les coordonnées du plaignant, et les renseignements éventuels pour une personne faisant un signalement au nom de quelqu'un d'autre;

[13] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html

(3) Information sur l'incident : un ou plusieurs incidents, y compris le numéro de l'incident, la description, les dates, les lieux, les événements, l'argent perdu, les éléments d'actif touchés, les méthodes de contact, les types de renseignements personnels à risque, les appareils concernés et les comptes de médias sociaux concernés;

(4) Information sur le suspect : aucune ou plusieurs descriptions de suspects, y compris des indices sur le suspect (p. ex. courrier électronique, téléphone, site Web, application);

(5) Fichiers de preuves : aucune ou plusieurs pièces jointes aux fichiers de preuves, y compris les descriptions et les attributs de métadonnées. Les types de fichiers pris en charge incluent, sans s'y limiter : HTML, JPEG, PDF, TXT, XLSX, XML, et PNG;

(6) Renvoi du numéro d'incident du signalement public avec un numéro de billet de la solution.

iv) Le site Web de signalement destiné au public publiera les fichiers complets de plaintes valides sur un service de file d'attente qui sera accessible à la solution.

v) Notez que la composante Site Web de signalement destiné au public devrait être déployée dans un conteneur au sein de l'espace infonuagique Protégé B de la GRC.

b) Exigences

i) L'entrepreneur doit fournir un moyen d'intégrer les données du site Web de signalement destiné au public dans la solution, en temps quasi réel, en utilisant un service de mise en file d'attente accessible dans l'espace infonuagique Protégé B de la GRC pour la communication.

ii) La solution de l'entrepreneur doit offrir la capacité d'abonnement au service de mise en file d'attente pour recevoir chaque fichier de plainte du site Web de signalement destiné au public, par l'entremise d'une API RESTful, afin que l'on puisse amorcer le traitement de triage automatisé.

4.5 Architecture cible

a) L'architecture cible est une illustration fondée sur les composantes qui décrit le flux d'information général entre les composantes pour illustrer les exigences de l'architecture de projet de la SNC (voir l'Appendice D – Diagramme de l'architecture conceptuelle générale). Le but de ce diagramme est de présenter un aperçu conceptuel destiné à aider l'entrepreneur à comprendre la vision de l'état final lors du développement de l'architecture de l'entrepreneur. L'entrepreneur doit fournir une conception fondée sur les composantes afin de faciliter la mise en œuvre et les besoins de soutien futurs du gouvernement du Canada.

4.6 Déploiement infonuagique

a) L'entrepreneur doit fournir une solution complète comprenant toute combinaison de modèles de services infonuagiques, y compris :

i. Solution interne gérée par la GRC (IaaS ou PaaS dans l'espace infonuagique protégé B de la GRC) avec octroi de licences perpétuelles – Solution déployée, exploitée et gérée par la GRC dans l'espace infonuagique Protégé B de la GRC en utilisant l'infrastructure du fournisseur de services d'infonuagique (FSI) applicable à la solution;

ii. SaaS ou PaaS publique – La solution sera hébergée et gérée par l'entrepreneur, sur le FSI choisi par l'entrepreneur, et utilisée par la GRC;

iii. Solution hybride de services infonuagiques – Une combinaison des modèles de services infonuagiques susmentionnés.

b) Les fournisseurs de services d'infonuagique doivent être intégrés avec succès dans le projet d'activation et de défense du nuage sécurisé (ADNS)[14] de Services partagés Canada et du SCT.

c) La solution doit être exempte de tout bogue critique et à forte incidence (critique étant défini comme un obstacle à l'exécution du travail et à forte incidence étant défini comme affectant gravement l'utilisation du système et nécessitant une correction dans la prochaine version), à jour et conforme aux spécifications décrites dans le présent document.

d) Pour garantir la conformité de la solution, il faut tenir compte des directives suivantes dans le cadre de l'architecture :

i) Le déploiement de la solution doit être entièrement automatisé à l'aide de modèles déclaratifs pour l'infrastructure sous forme de code dans un format respectant la norme de l'industrie.

ii) Les installations de logiciels de série doivent respecter les technologies de déploiement à l'échelle de la GRC (processus automatisés, configurations pouvant faire l'objet de scripts) (p. ex. les produits commerciaux installés sur un système d'exploitation Windows doivent utiliser Microsoft Endpoint Configuration Manager).

iii) L'entrepreneur ne doit utiliser que les services qui figurent sur la liste approuvée des services infonuagiques Protégé B fournis par le GC, ou les services pour lesquels le fournisseur a reçu une approbation écrite du Canada. Pour une liste complète des services infonuagiques Protégé B approuvés, veuillez consulter le catalogue des services de courtage infonuagique du GC[15] ou la demande d'arrangement en matière d'approvisionnement (DAMA-SaaS) de SPAC[16].

iv) La solution doit utiliser la fonctionnalité Azure AD (Active Directory) pour la gestion de l'identité et de l'accès pour les administrateurs de système (GRC et partenaires externes) de la solution.

(1) Identité et service principal gérés pour l'IaaS, la PaaS et le SaaS lorsqu'ils sont disponibles.

e) La solution doit mettre en œuvre les pratiques suivantes :

i) Gestion des clés ICP pour la gestion et le stockage des clés de chiffrement, des applications de code secret, des certificats et des jetons d'accès;

ii) Chiffrement, y compris le chiffrement du service de stockage, le chiffrement du disque et le chiffrement de la base de données avec la possibilité pour le Canada d'utiliser ses propres clés (fonctionnalité Utilisez votre propre clé comme Logiciel-service);

---

[14] https://wiki.gccollab.ca/L%27infocentre_de_l%27infonuagique

[15] https://cloud-broker.canada.ca/s/pbmmcatalogpage?language=fr

[16] https://www.tpsgc-pwgsc.gc.ca/app-acq/cral-sarc/saas-fra.html

iii) Le chiffrement utilisant « Pretty Good Privacy » (PGP) et x.509 doit être intégré de manière transparente pour prendre en charge la confidentialité cryptographique et l'authentification de la communication des données ainsi que la signature, le chiffrement et le déchiffrement des courriels et des fichiers pour accroître la sécurité de la communication par courriel avec les partenaires.

f) La solution doit satisfaire aux exigences de planification de la continuité des activités, de haute disponibilité et de redondance pour une mise en œuvre à l'échelle de l'entreprise. Ces exigences incluent la prise en charge de la redondance et du basculement en utilisant de nombreuses régions autorisées ou zones de disponibilité à l'intérieur du Canada.

g) La solution doit permettre la production de journaux (p. ex. activités, états, erreurs, événements) et des mesures (p. ex. consommation, échelles, performances) concernant les composantes individuelles qui forment l'écosystème de la solution. Les extrants des journaux et des mesures doivent être dans un format selon la norme de l'industrie et prendre en charge la diffusion en continu vers des paramètres de service précisés au sein de l'espace infonuagique Protégé B de la GRC.

h) Pour les instances de calcul de l'IaaS, les systèmes d'exploitation doivent être limités à Windows ou Linux (c.-à-d. Red Hat, SuSE ou Ubuntu) et prendre en charge l'automatisation des correctifs et des mises à jour, régulièrement.

i) L'entrepreneur doit compiler une liste détaillée des licences de logiciel et d'infrastructure qui seront nécessaires pour mettre en œuvre la solution, y compris les coûts annuels connexes pour la durée du contrat.

4.7 Code source et développement

a) L'entrepreneur doit, pour les parties de la solution qui supposent le développement de codes personnalisés et la configuration personnalisée, livrer une solution conformément aux directives suivantes :

i) l'entrepreneur doit fournir une équipe d'intégration qui travaillera en collaboration avec la GRC afin d'effectuer tous les travaux de développement à l'aide des postes de travail de la GRC, à partir des locaux de la GRC, ou au moyen d'une connexion à distance sécurisée (en fonction de l'incidence des restrictions liées à la COVID-19 qui peuvent être en vigueur) dans le cadre d'un abonnement distinct au sein de l'espace infonuagique Protégé B de la GRC;

ii) l'entrepreneur doit fournir une équipe d'intégration qui travaillera en collaboration avec le personnel du gouvernement du Canada afin de déployer les versions et les correctifs en vertu d'une entente de soutien avec le gouvernement du Canada;

iii) l'entrepreneur doit s'assurer que toutes les composantes d'intégration sont clairement décrites et sont fondées sur l'API avec un code personnalisé minimal. Tous les commentaires du code source doivent être écrits en anglais uniquement;

iv) l'entrepreneur doit développer des mises à jour et de nouvelles fonctionnalités dans un environnement de développement de l'espace infonuagique Protégé B de la GRC. La méthodologie utilisée doit respecter les Normes numériques du gouvernement du Canada, notamment en ce qui concerne la collaboration, l'intégration continue et le déploiement continu (CI/CD). L'entrepreneur doit diffuser l'information concernant l'installation et le soutien dans le cadre de séances de collaboration avec le gouvernement du Canada afin de maintenir un niveau élevé de compréhension des applications;

v) l'entrepreneur doit gérer le référentiel et le pipeline de code source dans un référentiel contrôlé par la GRC désigné. La GRC fournira des environnements de développement, d'essais/CQ et de production;

vi) l'entrepreneur doit regrouper le code logiciel et toutes ses dépendances afin qu'il puisse être exécuté de manière répétée et cohérente dans l'infrastructure de la solution. Cela doit permettre de développer des applications en écriture unique, exécutables n'importe où (WORA) dans une architecture de déploiement de conteneurs. Ces conteneurs doivent être contrôlés par version et inclure des scripts de déploiement. Des scripts d'installation, y compris des scripts d'annulation et des plans de récupération, sont requis pour toutes les versions;

vii) l'entrepreneur doit collaborer avec la GRC pour développer une pile technologique de développement et d'exploitation infonuagique (DevOps) de la GRC pour la solution qui soit compatible avec l'espace infonuagique Protégé B de la GRC;

viii) l'entrepreneur doit travailler en collaboration avec la GRC pour incorporer des scripts de sécurité dans la version afin de vérifier que chaque version est conforme à une liste convenue de contrôles de sécurité;

ix) l'entrepreneur doit fournir et maintenir une solution avec un ensemble complet d'essais unitaires et d'essais d'intégration automatisés de sorte que les essais d'application (à l'exclusion des essais d'accessibilité et des essais d'acceptation par l'utilisateur) soient complètement automatisés. L'entrepreneur doit également prendre en charge les essais des correctifs de maintenance et des mises à jour logicielles ainsi que les essais de régression pour s'assurer que les correctifs n'ont pas d'effet négatif sur les fonctionnalités existantes;

x) l'entrepreneur doit fournir des documents décrivant les principales méthodes de soutien, les plans de mise en œuvre et les processus de déploiement lors de l'intégration au sein de l'espace infonuagique Protégé B de la GRC. L'entrepreneur est également tenu de fournir des mises à jour des documents pendant le processus de version avant de passer à l'étape de la production.

4.8 Gestion de l'identité et de l'accès

a) La gestion de l'identité et de l'accès en ce qui concerne la solution se fera principalement à l'aide de Microsoft Azure Active Directory (Azure AD), comme il est expliqué en détail dans les sections suivantes. La solution doit permettre à l'équipe des activités liées à l'infonuagique de la GRC d'octroyer, de modifier et de révoquer l'accès en tant qu'administrateur de système à toutes les composantes de la SNC, par l'entremise du service Azure AD.

b) Bien que la responsabilité de la gestion du contenu d'Azure AD incombe à la GRC, l'entrepreneur doit configurer les composantes de la solution afin que cette dernière utilise Azure AD comme service de répertoire.

c) Les capacités de gestion de l'accès à la solution doivent être fournies à l'aide des rôles, des groupes, des identités et des attributs contenus dans le service Azure AD. L'entrepreneur peut demander d'apporter des modifications aux rôles, groupes, identités ou attributs Azure AD afin de répondre aux exigences de gestion de l'accès. L'entrepreneur doit soumettre une demande au gouvernement du Canada en fournissant les renseignements détaillés sur les éléments à ajouter et les raisons des modifications de la gestion de l'accès afin qu'une demande soit prise en considération.

d) La solution doit être capable de stocker et de gérer les certificats de clés publiques et privées (PGP et x.509) associés aux utilisateurs partenaires.

   i) Par exemple, lors de l'intégration, la solution doit prendre en charge la capture de la clé publique PGP de l'utilisateur partenaire (ou proposer de générer une paire de clés pour lui s'il n'en a pas), la stocker avec les détails du compte utilisateur et l'associer au courrier électronique de l'organisation concernée.

   ii) Dans le cas d'un employé de la GRC souhaitant générer une paire de clés PGP, la solution pourrait fournir un enveloppeur qui serait lié à un service de séquestre/récupération de clés et l'associerait à son identité de la GRC par courriel.

e) La solution doit être capable de fournir une fonctionnalité de connexion (authentification) conforme aux normes et technologies de gestion de l'identité approuvées par la GRC, au minimum à un niveau d'assurance 2 et à un niveau d'assurance 3 – comme l'indique le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3)[17].

f) La GRC fournira un moyen d'intégrer les justificatifs d'ICP de la GRC avec l'authentification à deux facteurs Azure AD. La solution doit garantir que toutes les décisions de contrôle d'accès utilisent le niveau d'assurance de la session d'authentification.

4.8.1 Gestion de l'identité et de l'accès pour l'administrateur de système

a) La solution doit utiliser Azure AD en ce qui concerne la gestion de l'identité et de l'accès pour l'administrateur de système (GRC et partenaires externes) de la solution.

b) La solution doit fournir une capacité de gestion de l'accès pour les comptes d'administrateur de système par l'entremise du contrôle d'accès fondé sur les rôles en utilisant les rôles définis dans la fonctionnalité Azure AD de la GRC.

[17] voir https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de

4.8.2 Gestion de l'identité et de l'accès pour le compte d'administration

a) La solution doit utiliser Azure AD en ce qui concerne la gestion de l'identité et de l'accès pour les comptes administratifs (notamment, mais sans s'y limiter, les identités gérées ou les comptes principaux de service) lorsqu'il est pris en charge, à l'exception des comptes autonomes, comme il est expliqué en détail dans la présente section.

b) La solution doit fournir une capacité de gestion de l'accès pour les comptes d'administration, à l'exception des comptes d'administration autonomes, par l'entremise du contrôle d'accès fondé sur les rôles en utilisant les rôles définis dans le schéma Azure AD de la GRC.

c) La création de tout compte d'administration autonome requis par la solution (tel que celui requis pour configurer une application permettant d'utiliser Azure AD) doit remplir toutes les conditions suivantes :

   i) Une demande d'utilisation du compte autonome contenant les applications et les ressources auxquelles on veut accéder en utilisant le compte, l'étendue des privilèges détenus par le compte, la méthode d'authentification utilisée pour le compte et la raison pour laquelle le compte est requis doit être fournie au gouvernement du Canada pour chaque compte individuel.

   ii) La demande d'utilisation du compte autonome doit être approuvée par le gouvernement du Canada avant d'être incluse dans la solution.

4.8.3 Composantes de gestion de l'accès de la SNC

a) Toutes les composantes de la solution doivent permettre un contrôle d'accès granulaire fondé sur les rôles en fonction des groupes et des attributs de la fonctionnalité Azure AD.

b) La solution doit avoir un contrôle d'accès granulaire qui permettra au gouvernement du Canada d'autoriser des activités génériques telles que la création, la lecture, la mise à jour, la suppression, ainsi que des capacités particulières pour les services individuels (telles que, mais sans s'y limiter, la présentation de demandes d'échange, de demandes de transfert de fichier).

c) L'entrepreneur doit travailler avec le gouvernement du Canada afin de fournir la granularité du contrôle d'accès nécessaire pour accorder le niveau d'accès approprié à chaque composante de chaque service aux utilisateurs internes et aux groupes partenaires qui y auront accès.

4.9 Journalisation et vérification

a) La fonctionnalité de gestion de l'information et des événements de sécurité (GIES) de la GRC doit avoir la capacité de regrouper et de corréler les journaux d'événements et de vérification de toutes les sources de journaux en ce qui concerne la gestion et la prestation de la solution. Le gouvernement du Canada se réserve le droit de déterminer, de hiérarchiser et, finalement, d'assimiler les messages d'événement, les messages d'information, les alertes et les alarmes. L'entrepreneur doit travailler avec le gouvernement du Canada pour configurer et gérer la quantité et le type d'enregistrements générés par la solution.

b) La solution de l'entrepreneur doit s'intégrer à la capacité de collecte des journaux de l'espace infonuagique Protégé B de la GRC.

c) L'entrepreneur doit travailler avec le gouvernement du Canada pour s'intégrer à la capacité de GIES de la GRC, y compris, mais sans s'y limiter, fournir les renseignements requis par le gouvernement du Canada et mettre en œuvre les configurations et les changements touchant la solution de l'entrepreneur. Les formats incluent le Common Event Format (CEF), Syslog et d'autres formats de journaux courants précisés par le gouvernement du Canada.

d) L'intégration doit se faire au moyen de flux de données fournis à la fonctionnalité de GIES de la GRC par l'une des méthodes suivantes ou les deux :

   i) les données des journaux sont transmises de l'entrepreneur à la capacité de collecte des journaux de l'espace infonuagique Protégé B de la GRC au moyen d'un format compatible avec la GIES de la GRC;

   ii) les données des journaux peuvent être récupérées à partir des systèmes de l'entrepreneur qui prennent en charge la récupération à distance à l'aide de la capacité de collecte de journaux de l'espace infonuagique Protégé B de la GRC.

e) L'entrepreneur doit fournir un mécanisme de gestion de la capacité des taux de transfert de données à la capacité de collecte de journaux de l'espace infonuagique Protégé B de la GRC afin de respecter les volumes approuvés par le gouvernement du Canada. Cela comprend, mais sans s'y limiter :

   i) Si les taux d'événements approchent d'une limite précisée par la GRC, l'entrepreneur doit travailler avec le gouvernement du Canada afin d'établir la raison de l'augmentation et prendre les mesures appropriées visant à annuler ou à corriger le changement.

f) L'entrepreneur doit fournir un mécanisme afin de s'assurer que les journaux de vérification peuvent être recueillis à partir de divers systèmes, fusionnés de manière centralisée et envoyés à la capacité de collecte de journaux de l'espace infonuagique Protégé B de la GRC pour être analysés régulièrement par un outil automatisé.

g) L'entrepreneur doit développer la capacité de journalisation de la solution afin de stocker de manière centralisée les événements de sécurité et ceux non liés à la sécurité ainsi que les traces de paquets de données dans la capacité de collecte de journaux de l'espace infonuagique Protégé B de la GRC.

h) La solution doit consigner les renseignements suivants pour toutes les activités de l'administrateur de système, y compris, mais sans s'y limiter :

   i) identifiant de l'administrateur système;

   ii) horodatage de l'activité;

   iii) détails relatifs à l'activité réalisée;

   iv) données modifiées par l'activité.

i) La solution doit assurer la journalisation des événements du compte d'administrateur de système suivants :

   i) création de compte;

   ii) modifications de compte;

   iii) désactivation de compte;

   iv) résiliation de compte;

v) authentification réussie;

vi) authentification infructueuse.

j) La solution doit fournir des renseignements de journalisation :

i) quel type d'événement de vérification s'est produit;

ii) quand (c.-à-d. la date et l'heure) l'événement de vérification s'est produit;

iii) le lieu de l'événement de vérification;

iv) la source de vérification de l'événement;

v) le résultat (c.-à-d. succès ou échec) de l'événement de vérification;

vi) l'identité de tout utilisateur et sujet lié à l'événement de vérification.

k) La solution doit consigner les événements suivants :

i) utilisation de comptes d'administrateur de système privilégiés;

ii) connexion et déconnexion de l'administrateur de système acceptées avec horodatage;

iii) tentatives de connexion refusées avec horodatage;

iv) connexion et déconnexion de l'administrateur de système ou de l'utilisateur acceptées avec horodatage;

v) octroi, modification ou révocation des droits d'accès, y compris l'ajout d'un nouvel administrateur de système, utilisateur ou groupe, la modification des niveaux de privilèges d'administrateur de système et d'utilisateur, la modification des accès aux fichiers, la modification des accès aux objets de base de données, la modification des règles de pare-feu et les modifications de mot de passe d'administrateur de système et d'utilisateur;

vi) changements de configuration, y compris l'installation de correctifs et de mises à jour logicielles ou d'autres modifications de logiciels installés;

vii) démarrage, arrêt ou redémarrage de processus;

viii) interruption, échec ou arrêt anormal de processus, plus particulièrement en raison de l'épuisement des ressources ou de l'atteinte d'un seuil ou d'une limite de ressources (comme pour l'unité centrale de traitement [UCT], la mémoire, les connexions réseau, la bande passante du réseau, l'espace disque ou d'autres ressources), la panne des services réseau comme le protocole de configuration dynamique des hôtes (DHCP) ou le système de noms de domaine (DNS) ou des pannes matérielles;

ix) détection d'activités suspectes ou malveillantes, par exemple à partir d'un système de détection d'intrusion au niveau de l'hôte ou d'un système de prévention des intrusions (SDI/SPI), d'un système antivirus ou d'un système anti-logiciels malveillants.

5. Plan de sécurité du système

a) L'entrepreneur doit examiner toutes les exigences de sécurité à l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité (MTES) et y répondre; il doit proposer un mécanisme pour répondre à l'exigence. En cas de conflit entre les exigences de l'ensemble de la DP et la MTES, la MTES aura préséance.

b) L'entrepreneur doit aborder tous les risques cernés par les processus de conformité du gouvernement du Canada, comme les vérifications, les activités liées à l'évaluation et autorisation de sécurité (EAS), les évaluations de la menace et des risques (EMR) et les évaluations des facteurs relatifs à la vie privée (EFVP).

c) L'entrepreneur doit permettre au gouvernement du Canada où à ses délégués, sans frais pour le gouvernement du Canada, d'accéder aux environnements de développement et d'essai au sein de l'espace infonuagique Protégé B de la GRC pour inspecter et vérifier la conformité de l'entrepreneur avec les exigences prévues au contrat en matière de confidentialité, de sécurité et de gestion de l'information, et d'avoir pleinement accès à l'ensemble des dossiers et renseignements personnels.

d) La solution doit permettre au gouvernement du Canada d'installer des prises d'accès réseau passives pour une capture réseau complète et soutenue de tout le trafic réseau de la couche IP (protocole Internet) et des interactions entre les composantes de la SNC avec la possibilité d'inspecter les données chiffrées.

e) L'entrepreneur doit collaborer aux inspections et aux vérifications de sécurité demandées par le gouvernement du Canada et fournir les preuves suivantes :

   i) les documents sur le flux de données et la description de la protection, de l'architecture et de la sécurité des données, pour ce qui a trait aux travaux prévus au contrat;

   ii) les plans de gestion des risques, les évaluations des risques et les EFVP propres à l'entrepreneur, pour ce qui a trait aux travaux prévus au contrat;

   iii) les entrevues des employés de l'entrepreneur et de tiers conseillers menées par le gouvernement du Canada au cours des heures de travail normales, ou bien en dehors de ces heures selon une entente mutuelle.

5.1 Exigences générales en matière de conformité

a) La SNC doit être protégée et sécurisée conformément aux politiques et aux lois du gouvernement du Canada en matière de sécurité. L'entrepreneur doit assurer la sécurité de la SNC conformément aux exigences en matière de sécurité continue ci-après.

5.1.1 Conformité avec les politiques du gouvernement du Canada

b) L'entrepreneur doit satisfaire aux politiques et aux lois du gouvernement du Canada en matière de sécurité qui régissent le traitement des renseignements protégé B, dont les mises à jour, les abandons ou les modifications, durant la période du contrat :

   i) GRC G1-009 – Transport et transmission de renseignements protégés ou classifiés[18].

[18] https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-fra.htm

5.1.2 Examen et certifications par des tiers

c) L'entrepreneur doit posséder des certifications valides et à jour de l'industrie du début à la fin du contrat :

   i) Norme ISO/IEC 27001:2013 Technologies de l'information – techniques de sécurité – exigences en matière de systèmes de gestion de la sécurité de l'information[19];

   ii) Norme ISO/IEC 27017:2015 Technologies de l'information – techniques de sécurité – code de pratique pour les contrôles de sécurité de l'information[20] fondée sur la norme ISO/IEC 27002:2013 Technologies de l'information – techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information des services infonuagiques;

   iii) Norme ISO/IEC 27018:2019 Technologies de l'information – techniques de sécurité – code de pratique pour la protection des renseignements permettant d'identifier une personne (RIP) dans les services infonuagiques publics utilisés comme processeur de RIP[21];

   iv) Rapport Service Organization Control (SOC) 2 Type II de l'AICPA pour les principes de confiance associés à la sécurité, à la disponibilité, à l'intégrité du traitement, à la protection des renseignements personnels et à la confidentialité, préparé par un comptable agréé indépendant.

d) Chaque rapport de certification ou de vérification fourni doit : (i) mentionner le nom légal de l'entreprise de l'entrepreneur ou du sous-processeur applicable; (ii) mentionner la date de certification de l'entrepreneur ou du sous-processus et l'état de cette certification; et (iii) dresser la liste des services visés par le rapport de certification. Si la méthode détachée est utilisée pour exclure des fournisseurs de sous-services (p. ex. service d'hébergement de données), le rapport d'évaluation du fournisseur de sous-services doit être inclus.

e) Chaque vérification doit faire l'objet d'un rapport à la disposition du Canada. Les certifications doivent être prouvées au moyen de pièces justificatives (p ex. rapport d'évaluation ISO préparé pour valider la conformité avec les normes ISO), et les rapports du vérificateur doivent contenir toute observation concrète. L'entrepreneur doit régler rapidement tout problème soulevé dans un rapport de vérification, à la satisfaction du vérificateur.

f) Tout rapport de vérification SOC 2 Type II doit être préparé dans les 12 mois précédant la date de début des opérations. Une lettre spéciale peut être fournie pour montrer que l'entrepreneur attend son renouvellement, s'il y a un écart entre la date du rapport du fournisseur de services et la fin de l'exercice de l'organisation utilisatrice (année civile ou fiscale)

g) L'entrepreneur doit conserver ses certifications ISO 27001, ISO 27017, ISO 27018 et SOC 2 Type II du début à la fin du contrat et fournir annuellement ou rapidement, à la demande du Canada, tous les rapports et les dossiers qu'il pourrait être raisonnable d'exiger en vue de démontrer que ses certifications sont valides et à jour.

---

[19] https://www.iso.org/standard/54534.html

[20] https://www.iso.org/standard/43757.html

[21] https://www.iso.org/standard/43757.html

5.1.3 Programme d'évaluation de la sécurité des TI du fournisseur de services infonuagiques

a) Si, durant le contrat et après l'approbation de l'autorité responsable du projet, l'entrepreneur fait migrer l'application ou des données d'un lieu physique à une solution infonuagique, il doit démontrer que le fournisseur de services infonuagiques :

   i) satisfait aux exigences en matière de sécurité énoncées dans le Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage[22] qui visent les services infonuagiques utilisés pour la SNC;

   ii) a fait l'objet d'une évaluation dans le cadre du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques du Centre canadien pour la cybersécurité (ITSM.50.100)[23].

b) Tout fournisseur de services infonuagiques qui a participé au processus doit confirmer au moyen de documents qu'il a terminé le processus d'évaluation, soit : (i) une copie du dernier rapport d'évaluation fourni par le CCCS; ou (ii) une copie du dernier résumé de rapport fourni par le CCCS.

5.1.4 Gestion des risques liés à la chaîne d'approvisionnement

a) L'entrepreneur doit disposer de mesures de protection pour atténuer les risques et les vulnérabilités liés à la chaîne d'approvisionnement qui touchent les services de TI afin d'assurer la sécurité des systèmes d'information et des éléments de TI utilisés pour fournir les services. Cela inclut, sans s'y limiter, l'élaboration et la prise de mesures pour atténuer et contenir les risques associés à la sécurité des données par une séparation appropriée des tâches, un contrôle d'accès basé sur les rôles et des droits d'accès minimaux pour tout le personnel, y compris les sous-traitants de la chaîne d'approvisionnement.

b) L'entrepreneur doit tenir un plan de gestion des risques liés à la chaîne d'approvisionnement décrivant son approche à cet égard et la façon dont elle lui permet d'atténuer ces risques.

c) L'approche de gestion des risques liés à la chaîne d'approvisionnement doit être harmonisée avec une des pratiques exemplaires suivantes :

   i) ISO/IEC 27 036 Technologies de l'information – techniques de sécurité – sécurité de l'information dans le contexte des relations avec les fournisseurs (partie 1 de 4);

   ii) Publication spéciale de la NIST 800-161 – Pratiques de gestion des risques liés à la chaîne d'approvisionnement pour les organisations et les systèmes d'information fédéraux.

[22] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html

[23] https://cyber.gc.ca/sites/default/files/publications/itsm.50.100-fr.pdf

5.2 Examen de la conformité

a) Le Canada effectuera, chaque année, une vérification et un examen de la conformité approuvés par le gouvernement du Canada – payés par l'entrepreneur – qui comprennent, mais sans s'y limiter :

   i) l'assurance que la solution est conforme aux exigences de sécurité de la SNC (voir l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité) et au profil de contrôle de sécurité ministériel (PCSM) de la GRC, y compris un examen du plan d'action et des jalons visant à s'assurer que les jalons sont atteints;

   ii) l'assurance que tous les logiciels de la solution possèdent une version à jour et actuelle des mises à jour et des correctifs de sécurité pour toutes les vulnérabilités connues;

   iii) la vérification que l'entrepreneur surveille de façon proactive les vulnérabilités des logiciels de la SNC et qu'il installe tout correctif de sécurité et toute nouvelle version des logiciels nécessaire à la correction de ces vulnérabilités;

   iv) la composition de l'équipe de base de l'entrepreneur.

b) L'entrepreneur doit fournir les pièces justificatives requises dans les dix (10) jours ouvrables suivant une demande présentée par le gouvernement du Canada dans le cadre de l'examen de la conformité.

c) Si le Canada juge que les pièces justificatives ne démontrent pas le respect du contrat, il demandera à l'entrepreneur un plan dressant les mesures qu'il prendra pour régler les écarts relevés par rapport aux conditions générales du contrat.

5.3 Validation de sécurité

a) L'entrepreneur doit remettre au Canada une MTES offrant un suivi à l'égard de chaque exigence d'assurance de la sécurité de la SNC marquée aux fins de validation dans l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité. Pour chaque exigence, la MTES doit indiquer des renvois à des documents de conception des services, qui décrivent les mesures de sécurité à mettre en œuvre. La matrice permet de s'assurer que la conception générale des services répond pleinement aux exigences en matière de sécurité.

b) Il faut joindre à la MTES présentée au gouvernement du Canada tous les documents portant sur les services auxquels elle renvoie. Ceux-ci doivent décrire les mesures de sécurité avec suffisamment de détails pour permettre au gouvernement du Canada de confirmer qu'elles répondent aux exigences qui sont énoncées dans l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité de la SCN.

c) L'entrepreneur doit travailler en collaboration avec la GRC pour évaluer la solution par rapport au PCSM de la GRC dans le cadre du processus d'EAS.

5.4 Sécurité des systèmes et des données de l'environnement

5.4.1 Attestation de sécurité des installations

a) Tout au long des travaux, l'entrepreneur doit posséder une attestation de sécurité de niveau protégé B pour toutes les installations primaires, secondaires et de reprise après sinistre où sont hébergées, entreposées ou traitées des données de la SNC, conformément à la Directive sur la gestion de la sécurité du gouvernement du Canada[24].

5.4.1.1.1 *Sécurité matérielle*

a) L'entrepreneur doit maintenir des mesures de sécurité matérielle en vue de protéger les installations de TI et les systèmes d'information qui contiennent et traitent des données de la SNC des accès non autorisés, des altérations, des pertes, des dommages et des saisies, et ses mesures doivent être fondés sur une approche de la sécurité matérielle axée sur la prévention-détection-intervention-récupération. À tout le moins, l'approche doit inclure les éléments suivants :

i) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'un centre de données n'empêche pas la récupération des données conformément au niveau de service prescrit;

ii) l'utilisation adéquate des supports de TI;

iii) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue;

iv) le contrôle de l'accès aux dispositifs de sortie et d'entreposage des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada;

v) la restriction de l'accès physique aux actifs des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, validé par deux formes d'identification;

vi) l'escorte des visiteurs et la surveillance de leurs activités;

vii) la tenue de registres de vérification de l'accès physique;

viii) le contrôle et la gestion des dispositifs d'accès physique;

ix) l'application de mesures de protection des données de la SNC à d'autres lieux de travail (p. ex. les sites de télétravail);

x) la consignation et la surveillance de tous les accès physiques aux installations des centres de données et de tous les accès par voie électronique aux composants des systèmes d'information qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.

Source : Directive sur la gestion de la sécurité du gouvernement du Canada[25].

---

[24] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611&section=html

[25] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611&section=procedure&p=C

h) Les installations de l'entrepreneur doivent être dotées de mesures de protection physique appliquées conformément aux directives et aux normes en matière de sécurité matérielle de la GRC, particulièrement le guide G1-025 – Protection, détection et intervention[26].

i) L'entrepreneur doit aviser l'autorité responsable du projet et la Direction des services de la sécurité du personnel (anciennement la DSIC) de toute amélioration ou modification apportée aux installations qui gèrent la SNC.

5.4.2 Zones de sécurité

a) L'entrepreneur doit utiliser des contrôles de sécurité afin d'assurer un isolement approprié des ressources, afin que les données de la SNC ne se retrouvent pas mêlées à celles d'autres locataires, et ce, pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système du service. Cela comprend les contrôles d'accès et le renforcement des mesures d'isolement logique et physique afin d'assurer :

   i) la séparation de l'administration interne de l'entrepreneur des ressources utilisées par ses clients;

   ii) la séparation des ressources des clients dans les environnements multilocataires afin d'empêcher que les activités d'un client malveillant ou compromis aient des répercussions sur le service ou les données d'un autre.

b) L'entrepreneur doit veiller à ce que les zones de sécurité du réseau soient toujours harmonisées avec :

   i) les Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du Centre de la sécurité des télécommunications (CST)[27];

   ii) les Considérations de conception relatives au positionnement des services dans les zones (ITSG-38) du CST[28].

c) L'entrepreneur doit veiller à la surveillance et à la maintenance des zones de sécurité du réseau pour :

   i) Assurer un contrôle rigoureux de toutes les interfaces des zones publiques, y compris tous les réseaux externes non contrôlés comme Internet, à un périmètre de sécurité déterminé;

   ii) appliquer des mesures de protection et de défense périmétrique (p. ex. pare-feu, routeurs) pour intercepter tout le trafic et protéger les serveurs qui sont accessibles par Internet.

d) Du début à la fin du contrat, tout changement prévu ou non prévu à l'environnement doit être documenté et faire l'objet d'une mise à jour, conformément au plan de gestion du changement et aux processus connexes.

---

[26] http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-025-fra.htm

[27] https://cyber.gc.ca/fr/orientation/exigences-de-base-en-matiere-de-securite-pour-les-zones-de-securite-de-reseau-au-sein2

[28] https://www.cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones

5.4.3 Examen de la conception des services

a) La conception des services pour la SNC doit être examinée et approuvée par le Canada. L'entrepreneur doit notamment fournir au Canada une copie de l'architecture proposée pour la SNC, qui permettra au Canada d'examiner :

   i) les mesures de protection et de sécurité et les éléments de sécurité proposés qui seront appliqués dans le cadre de la SNC;

   ii) la configuration et la fiabilité de tous les dispositifs de sécurité.

5.4.4 Protection contre les maliciels

a) L'entrepreneur doit protéger des cyberattaques les éléments de TI utilisés pour mettre en application et gérer la solution, notamment en surveillant les dispositifs, les serveurs, les périphériques et les postes de travail, ainsi qu'empêcher toute source externe d'y pénétrer.

e) La protection du réseau est nécessaire et elle doit être maintenue afin de pouvoir détecter et éliminer les logiciels malveillants ou les tentatives de connexion au réseau qui proviennent de l'extérieur et qui ne sont pas autorisées.

f) L'entrepreneur doit procéder au balayage de l'environnement hébergeant la SNC afin de détecter la présence de maliciels. Des mécanismes actifs de protection de l'hôte doivent être intégrés aux serveurs qui effectuent :

   i) le balayage de maliciels à l'accès;

   ii) le balayage actif et périodique de maliciels au moins une fois par mois.

5.4.5 Mises à jour de sécurité

a) L'entrepreneur doit effectuer les mises à jour de sécurité des systèmes d'exploitation et des applications afin de corriger les vulnérabilités au moyen d'une approche axée sur les risques et harmonisée avec la méthode figurant dans le document Correction des systèmes d'exploitation et des applications – Bulletin de sécurité des TI à l'intention du gouvernement du Canada (ITSB-96) du Centre de la sécurité des télécommunications[29].

5.4.6 Gestion des correctifs et des vulnérabilités

a) Pour gérer les correctifs, l'entrepreneur doit au moins effectuer ce qui suit :

   iii) s'assurer qu'une version prise en charge et à jour des applications et des systèmes d'exploitation est utilisée;

   iv) veiller à ce que les vulnérabilités soient évaluées et à ce que les correctifs de sécurité fournis par le fournisseur soient appliqués rapidement;

   v) établir l'ordre de priorité des correctifs et des ensembles de modifications provisoires critiques à l'aide d'une approche fondée sur le risque;

   vi) faire des mises à l'essai et des vérifications pour s'assurer que les correctifs ont été appliqués correctement.

[29] https://cyber.gc.ca/fr/orientation/correction-des-systemes-dexploitation-et-des-applications-bulletin-de-securite-des-ti

5.4.7 Gestion des privilèges

a) L'entrepreneur doit gérer et surveiller les accès privilégiés à la SNC pour s'assurer que les interfaces de service sont protégées contre les accès non autorisés. Ce processus doit, au minimum :

i) permettre le renforcement et la vérification des autorisations d'accès aux données de la SNC;

ii) restreindre et minimiser l'accès seulement aux appareils autorisés et aux utilisateurs et aux administrateurs ayant explicitement besoin de cet accès;

iii) restreindre tout l'accès aux interfaces de service qui hébergent des données de la SNC aux personnes ayant un identifiant, une authentification et une autorisation uniques;

iv) mettre en place des mécanismes d'authentification à facteurs multiples pour authentifier les utilisateurs ayant des privilèges d'accès;

v) mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux données de la SNC;

vi) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, ainsi que les rôles de développement des rôles opérationnels, et les rôles de gestion de l'accès des autres rôles opérationnels;

vii) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux employés et aux entrepreneurs;

viii) utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services et de l'infrastructure;

ix) mettre en place un processus automatisé ou manuel pour effectuer une vérification périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes, au minimum – si un processus manuel de vérification est utilisé, la politique ou la procédure connexe doit être documentée et transmise au Canada;

x) révoquer, en cas de cessation d'emploi ou de contrat, les authentifiants et les justificatifs d'accès associés à l'employé ou au sous-traitant.

5.4.8 migration et échange de données sécurisés

a) L'entrepreneur doit appliquer les pratiques de migration de données ci-dessous pour soutenir la mise en œuvre de la SNC :

vii) **Entre l'entrepreneur et ses sous-traitants**

L'entrepreneur doit utiliser la solution de transfert sécurisé de fichiers (MSFT)[30] approuvée par le gouvernement du Canada pour la migration et l'échange sécurisé de données entre lui-même et ses sous-traitants (le cas échéant), qui prend en charge le protocole Hypertext Transfer Protocol Secure (HTTPS), File

[30] http://sftweb.pwgsc.gc.ca/sft-html/Documents_f.html

Transfer Protocol over Secure Socket Layer (FTPS) et File Transfer Protocol over Secure Shell (SFTP) et comprend un système de cryptographie conforme à la norme Federal Information Processing Standard (FIPS 140-2).

viii) **Entre l'entrepreneur et le Canada**

L'entrepreneur doit établir des connexions réseau sécurisées appliquant le protocole TLS 1.2 ou une version subséquente, qui utilisent les algorithmes cryptographiques et les certificats approuvés par le Centre de la sécurité des télécommunications :

- Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062)[31] du CST, section 3.1 sur les suites de chiffrement TLS;
- Algorithmes cryptographiques pour l'information non classifiée, protégé A et protégée B (ITSP.40.111)[32] du CST.

L'entrepreneur doit tenir à jour ses connexions réseau sécurisées conformément aux exigences du CST, qui pourraient évoluer au cours du contrat.

ix) **Entre l'entrepreneur et un tiers**

Après avoir obtenu l'approbation de l'autorité responsable du projet et de la Division de filtrage de la sécurité du personnel (anciennement la DSIC), l'entrepreneur doit fournir un outil ou une méthode de transfert de données sécurisé lui permettant de transférer des données à un tiers approuvé afin de faciliter les vérifications externes et d'autres projets lancés par le gouvernement.

5.4.9 Protection cryptographique

a) L'entrepreneur doit utiliser des mesures de protection cryptographique et les mettre à jour, si cela est jugé nécessaire après discussion avec le Canada, afin d'assurer la protection des données personnelles ou des mesures de protection de l'intégrité dans le cadre du mécanisme d'authentification (p. ex. solutions VPN, TLS, modules logiciels, ICP, jetons d'authentification, le cas échéant) utilisé pour le service.

b) L'entrepreneur doit utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques et des cryptopériodes approuvés, ce qui comprend :

i) des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui ont été approuvés par le Centre de la sécurité des télécommunications et validés par le Programme de validation des algorithmes cryptographiques[33] du NIST et qui sont précisés dans le document ITSB-111 ou dans une version ultérieure;

[31] https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp400622

[32] https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b

[33] https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

ii) une mise en œuvre et une utilisation dans un mode approuvé d'un module cryptographique validé par le Programme de validation des modules cryptographiques[34] du NIST et qui répond au moins aux exigences du NIST en matière de sécurité des modules cryptographiques (FIPS 140-2)[35] de niveau 1. Au minimum, une cryptographie conforme à la norme FIPS 140-2 et validée doit être utilisée pour les dispositifs de protection du périmètre et partout où le chiffrement est requis.

5.4.10 Sécurité de l'échange de données informatisées

a) L'entrepreneur doit s'assurer que les données de la SNC fournies ou échangées entre le GNCC et des partenaires au moyen de l'EDI ou d'autres services numériques répondent à toutes les exigences en matière de sécurité de la SNC.

b) La solution de l'entrepreneur doit permettre la transmission sécurisée de renseignements par EDI entre les partenaires et le GNCC.

c) La solution de l'entrepreneur doit protéger l'intégrité et l'authenticité de l'ensemble des données de la SNC, qu'elles soient entreposées ou en mouvement. Elle doit aussi protéger les données contre la corruption et les modifications accidentelles ou malveillantes au moyen de hachage, de certificats numériques ou de technologies similaires, conformément à la norme 5.4.10 sur la protection cryptographique.

d) L'entrepreneur doit s'assurer que la sécurité et la protection de l'information sont maintenues au moment de la conversion ou du téléchargement de données.

5.4.11 Stockage et conservation des données

a) L'entrepreneur doit conserver toutes les données de récupération de la SNC conformément aux exigences du GNCC en matière de conservation de l'information et aux suivantes :

iii) toute manipulation de supports de stockage de données portatifs pouvant être utilisés avec le système doit être conforme aux exigences en matière d'étiquetage, de destruction, de manipulation et d'entreposage de ces biens énoncées dans l'avis Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada (AMPTI 2014-01)[36];

iv) toutes les données de récupération doivent être conservées à un endroit sûr et à l'abri des incendies et des inondations;

v) les mesures de protection et de conservation des données doivent satisfaire à la norme Advanced Encryption Standard (AES), avec des longueurs de clé de 128 bits, afin d'assurer la protection et l'intégrité des données de récupération au lieu de stockage;

---

[34] https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

[35] https://csrc.nist.gov/publications/detail/fips/140/2/final

[36] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/avis-mise-oeuvre-politique/utilisation-securisee-stockage-donnees-portatifs-gouvernement.html

vi) l'entrepreneur doit vérifier s'il est possible de réutiliser en toute sécurité un dispositif de stockage, selon les lignes directrices du CST sur le nettoyage des supports de TI (ITSP.40.006)[37];

vii) l'entrepreneur est responsable des coûts associés à toute destruction de données amorcée par lui et approuvée par l'autorité responsable du projet.

5.4.12 Extraction de données

a) L'entrepreneur doit fournir les outils et les services nécessaires pour que le Canada puisse :

viii) extraire toutes les données en ligne, pseudo-directes et hors ligne du Canada, y compris, au minimum, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités infonuagiques, les codes source hébergés dans un référentiel de codes du Canada et les configurations réseau, de sorte que tout utilisateur final du Canada puisse se servir de ces instructions pour effectuer la migration d'un environnement à un autre;

ix) effectuer le transfert sécurisé de toutes les données du Canada, y compris les données de contenu et les métadonnées connexes, dans un format lisible et utilisable par machine (y compris le format CSV) et conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue de Bibliothèque et Archives Canada[38].

5.4.13 Destruction des données

a) À la fin de la période du contrat (c.-à-d. à l'expiration ou à la résiliation du contrat) ou à la demande de l'autorité responsable du projet, l'entrepreneur doit suivre les lignes directrices du CST sur le nettoyage des supports de TI (ITSP.40.006)[39] contenant des données de la SNC.

c) L'entrepreneur doit prouver à l'aide de pièces justificatives, comme un certificat, que toutes les données d'utilisateur associées à la SNC ont été détruites.

d) L'entrepreneur est responsable de tous les coûts liés à la destruction de supports ayant contenu de l'information protégé B de la SNC.

5.4.14 Transport des données

a) Si des données en format papier doivent être transportées physiquement, l'entrepreneur doit respecter le guide de la GRC G1-009 – Transport et transmission de renseignements protégés ou classifiés[40] et le Manuel de la sécurité des contrats[41] – Chapitre 6 : Manipulation et protection de renseignements et de biens.

---

[37] https://www.cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006

[38] https://www.bac-lac.gc.ca/fra/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx

[39] https://www.cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006

[40] https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-fra.htm

[41] https://www.tpsgc-pwgsc.gc.ca/esc-src/msc-csm/chap6-fra.html

b) L'entrepreneur doit marquer tous les documents en format papier et les autres supports de la classification de sécurité appropriée la plus élevée, selon l'autorité responsable du projet.

c) L'entrepreneur doit obtenir l'approbation de l'autorité responsable du projet avant d'entrer ou de sortir des données de leur emplacement physique protégé B.

5.5 Accès utilisateur autorisé

5.5.1 Attestation de sécurité du personnel

a) L'entrepreneur doit s'assurer que toutes les personnes qui traitent, consultent, gèrent ou sont en contact avec des données de la SNC ou qui ont accès aux installations de la SNC ont une attestation de sécurité valide, soit une cote de fiabilité ou un niveau de sécurité supérieur, selon les exigences du gouvernement du Canada en matière de niveaux de sécurité[42]. L'entrepreneur doit également s'assurer que les nouveaux membres du personnel, y compris les sous-traitants, possèdent les attestations appropriées et qu'ils les conservent tout au long du contrat.

e) L'entrepreneur doit s'assurer que les mesures de vérification du personnel sont appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité[43] du gouvernement du Canada afin de protéger adéquatement les renseignements protégé B.

5.5.2 Contrôles d'accès

a) L'entrepreneur doit prévoir des mesures de contrôle d'accès basé sur les rôles comme suit :

   i) l'entrepreneur doit intégrer des contrôles d'accès basés sur les rôles définis dans la SNC – chaque rôle se voit attribuer des capacités et un accès en fonction du droit d'accès minimal requis pour ce rôle et du besoin de savoir;

   ii) l'entrepreneur doit mettre en œuvre un processus pour gérer les comptes uniques de tous les utilisateurs de la SNC autorisés par l'autorité responsable du projet, de ses données protégé B ou, à tout le moins, des interfaces du P3 et de la SNC;

   iii) l'entrepreneur doit apporter aux profils d'accès utilisateur les changements demandés dans les trois jours suivant la réception de la demande de l'autorité responsable du projet.

f) L'entrepreneur doit mettre en œuvre des mécanismes d'authentification à facteurs multiples pour les utilisateurs et les comptes privilégiés.

g) L'entrepreneur doit s'assurer que les mots de passe répondent aux exigences du Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031)[44] du CST.

h) La page de confirmation de la connexion de la SNC doit indiquer la date et l'heure de la dernière connexion réussie.

---

[42] https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html

[43] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115

[44] https://www.cse-cst.gc.ca/fr/node/2454/html/28582

i) Tout changement apporté à un compte utilisateur doit être accompagné d'un document de contrôle indiquant la nature du changement, le compte utilisateur à l'origine du changement, ainsi que la date, l'heure et l'auteur du changement.

j) L'entrepreneur doit tenir à jour ses contrôles et accès utilisateurs, selon les changements au sein du personnel, et aviser l'autorité responsable du projet de tout changement à cet égard.

5.5.3 Protection des comptes

a) L'entrepreneur doit appliquer des contrôles pour la génération de mots de passe et la mise à jour des mots de passe existants qui s'harmonisent l'un ou l'autre des éléments suivants :

i) le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031)[45] du CST;

ii) d'autres pratiques exemplaires de l'industrie, comme la norme ISO 27001 ou celles du NIST.

5.5.4 Sensibilisation à la sécurité et formation

a) L'entrepreneur doit fournir une formation de sensibilisation à la sécurité ou une séance d'information afin que tous les membres du personnel (y compris les sous-traitants) qui traitent des renseignements protégé B de la SNC comprennent leur rôle et leurs responsabilités quant à la gestion de la sécurité de l'information avant de commencer à utiliser la SNC.

5.6 Essai des mécanismes de sécurité

a) L'entrepreneur doit présenter au Canada un plan d'essai des mécanismes de sécurité qui documente les jeux d'essai destinés à vérifier chaque exigence d'assurance de la sécurité de l'environnement de production de la SNC (EP de la SNC), marqué aux fins d'essai des mécanismes de sécurité à l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité.

b) L'entrepreneur doit exécuter le plan d'essai des mécanismes de sécurité à l'égard de chaque mesure de sécurité et présenter au gouvernement du Canada un rapport sur les essais des mécanismes de sécurité qui satisfait à une ou plusieurs des exigences de sécurité marquées aux fins d'essai des mécanismes de sécurité à l'Appendice E – La matrice de traçabilité des exigences en matière de sécurité.

i) les procédures d'essai doivent confirmer que les mécanismes de sécurité sont mis en œuvre correctement et qu'ils respectent les normes applicables précisées dans les spécifications de la conception du service;

ii) les résultats prévus et ceux obtenus pour chaque procédure d'essai des mécanismes de sécurité;

iii) une description des mesures correctives apportées à l'EP de la SNC pour chacun des écarts constatés par rapport aux résultats prévus ayant pu être corrigés au moment de la vérification;

[45] https://www.cse-cst.gc.ca/fr/node/2454/html/28582

iv) un renvoi à une demande de modification de chacun des écarts par rapport aux résultats prévus n'ayant pu être corrigés au moment de la vérification (p. ex. parce que la correction aurait entraîné des modifications plus importantes).

b) L'entrepreneur doit mettre à jour la MTES afin d'inclure le suivi entre les exigences de sécurité marquées aux fins d'essai des mécanismes de sécurité et les procédures d'essai.

c) L'entrepreneur doit permettre au gouvernement du Canada d'assister à l'essai des mécanismes de sécurité, ce qui comprend la possibilité d'observer les représentants de l'entrepreneur pendant qu'ils exécutent les procédures d'essai des mécanismes de sécurité ou la capacité de consulter les résultats du journal d'essai lorsque l'essai des mécanismes de sécurité est automatisé.

5.7 Méthodes d'évaluation des contrôles de sécurité

a) L'entrepreneur doit utiliser les méthodes d'évaluation des contrôles de sécurité suivantes dans le rapport d'essai et d'évaluation des mécanismes de sécurité :

i) MÉTHODE D'ÉVALUATION : Examen :

(1) OBJETS VISÉS PAR L'ÉVALUATION :

a) Spécifications (p. ex. politiques, plans, procédures, exigences du système, conceptions);

b) Mécanismes (p. ex. fonctionnalité mise en œuvre dans le matériel, logiciel, micrologiciel);

c) Activités (p. ex. opérations, administration, gestion du système; exercices).

(2) DÉFINITION : La vérification, l'inspection, la revue, l'observation, l'étude ou l'analyse d'un ou de plusieurs objets pour faciliter la compréhension, apporter des éclaircissements ou obtenir des données probantes; les résultats contribuent à déterminer l'existence, la fonctionnalité, l'exactitude, l'exhaustivité et la possibilité d'amélioration des contrôles de sécurité au fil du temps;

ii) MÉTHODE D'ÉVALUATION : Essai :

(1) OBJETS VISÉS PAR L'ÉVALUATION :

a) Mécanismes (p. ex. matériel, logiciel, micrologiciel);

b) Activités (p. ex. opérations, administration, gestion du système; exercices).

(2) DÉFINITION : La mise à l'essai d'un ou de plusieurs objets dans des conditions précises pour comparer le rendement réel avec le rendement souhaité; les résultats contribuent à déterminer l'existence, la fonctionnalité, l'exactitude, l'exhaustivité et la possibilité d'amélioration des contrôles de sécurité au fil du temps.

5.8 Évaluation des vulnérabilités

a) L'entrepreneur doit permettre que les essais d'évaluation des vulnérabilités internes soient réalisés au fur et à mesure des besoins par le gouvernement du Canada, l'entrepreneur ou un tiers choisi par le gouvernement du Canada ou par l'entrepreneur. Ces essais d'évaluation doivent être réalisés au minimum chaque année et alignés sur les contrôles de gestion des vulnérabilités dans le PCMS. L'entrepreneur doit déterminer l'attribution de la responsabilité liée au soutien des essais d'évaluation des vulnérabilités.

b) Si l'entrepreneur choisit de permettre au Canada de réaliser les essais d'évaluation des vulnérabilités internes, l'entrepreneur doit fournir :

   i) l'accès logique à l'espace infonuagique Protégé B de la GRC où l'infrastructure de l'environnement d'essai de la SNC (EE de la SNC) est située et exploitée;

   ii) l'accès réseau (ou les accès, s'il y a lieu) à l'EE de la SNC afin de permettre l'analyse du réseau et des périphériques hôtes;

   iii) l'aide d'au moins un (1) membre du personnel technique qui connaît bien les aspects techniques de l'infrastructure de l'EE de la SNC (c.-à-d. le matériel et les produits du réseau, ainsi que leur configuration) pendant la partie des essais d'évaluation des vulnérabilités internes réalisés.

c) Si l'entrepreneur (ou un tiers agissant au nom de l'entrepreneur) décide de mener ses propres essais d'évaluation des vulnérabilités internes, il doit :

   i) soumettre un plan d'évaluation des vulnérabilités au gouvernement du Canada pour approbation préalable;

   ii) inclure dans la portée du plan l'analyse de l'ensemble du réseau et des périphériques hôtes déployés dans l'EE de la SNC;

   iii) réaliser les essais d'évaluation des vulnérabilités dans l'EE de la SNC;

   iv) fournir les résultats au gouvernement du Canada pour examen et analyse. Le gouvernement du Canada peut exiger la mise en œuvre des changements initiés par l'entrepreneur en fonction d'un examen et d'une analyse.

d) Le gouvernement du Canada peut réaliser des essais d'évaluation des vulnérabilités externes par rapport à l'EE de la SNC et fournir à l'entrepreneur un rapport d'évaluation des vulnérabilités qui indiquera les vulnérabilités détectées par le gouvernement du Canada.

e) L'entrepreneur doit présenter au gouvernement du Canada un rapport sur l'atténuation des vulnérabilités qui comprend :

   i) une liste de vulnérabilités pour lesquelles le gouvernement du Canada recommande la mise en œuvre de mesures correctives;

   ii) une liste des vulnérabilités pour lesquelles l'entrepreneur recommande la mise en œuvre de mesures correctives s'il a choisi de mener ses propres essais d'évaluation des vulnérabilités internes;

   iii) une description des mesures correctives à mettre en œuvre qui comprend les délais prévus;

   iv) les documents sur les services mentionnés dans la MTES qui doivent être mis à jour en raison de la mise en œuvre de mesures correctives.

f) L’entrepreneur doit mettre en œuvre les mesures correctives indiquées dans le rapport d’atténuation des vulnérabilités approuvé dans le délai qui y est établi.

6. Gestion de projet

6.1 Contexte

a) Actuellement, le gouvernement du Canada utilise une méthodologie de gestion de projet conforme à la Directive sur la gestion de projets et programmes (en vigueur en avril 2019) du gouvernement du Canada[46].

b) Le Canada gérera la réalisation du projet de la SNC selon une approche hybride de gestion de projet qui intègre les méthodes Agile à la méthodologie de gestion de projet existante de la GRC. Les bases de référence théoriques pour la portée, le calendrier et le coût du projet seront définies avec suffisamment de flexibilité pour tenir compte des principes de développement itératifs et dynamiques de l'entrepreneur. Ces bases de référence théoriques permettront de suivre les progrès, de mesurer la performance et d'entreprendre toute action corrective.

6.2 Approche liée à la gestion du déploiement de la solution

a) Le Canada s'attend à ce que la méthode de développement et d'intégration du système de l'entrepreneur englobe les interactions entre l'entrepreneur et le client d'affaires de la GRC qui possède et tient à jour le carnet de produit. Le client d'affaires de la GRC peut redéfinir les priorités du contenu du carnet de produit comme bon lui semble.

b) L'entrepreneur doit travailler avec le client d'affaires de la GRC afin de déterminer les fonctionnalités les plus importantes au début de chaque sprint (versions successives ou livraison de fonctionnalités), ainsi que tous les détails nécessaires à l'entrepreneur pour mettre en œuvre ces fonctionnalités. L'entrepreneur doit estimer les travaux et s'engager seulement à l'égard de ce qu'il peut faire pendant le sprint. Les modifications ne seront autorisées pendant le sprint que si elles sont approuvées par le gouvernement du Canada dans le cadre du processus officiel d'autorisation de changement. Pendant le développement des fonctionnalités de sprint en vue du déploiement, le client d'affaires de la GRC, en collaboration avec l'entrepreneur, sélectionnera le prochain ensemble de fonctionnalités pour le prochain sprint.

c) Tout changement important ou toute suppression d'une portée obligatoire doit avoir lieu dans le cadre d'autorisations officielles de changement, conformément au processus de gestion du changement approuvé, décrit dans le produit livrable du plan de gestion de projet de l'entrepreneur.

d) Les activités du projet de SNC doivent être ordonnées, et les caractéristiques du produit seront classées en fonction des besoins et des priorités du client d'affaires de la GRC. Il est prévu que les fonctionnalités de la solution seront développées dans de nombreux sprints au cours desquels les équipes exécutent des tâches qui peuvent être accomplies dans un délai défini.

e) Les versions et sprints doivent développer continuellement les fonctionnalités répertoriées dans le carnet de produit qui ont été classées par ordre de priorité en collaboration avec le client d'affaires jusqu'à ce que la pleine capacité opérationnelle soit atteinte à la fin du contrat.

[46] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32594

f) La progression et le rendement d'ensemble du projet seront examinés à divers points de contrôle planifiés auprès d'un public plus large afin que l'on puisse recueillir des préoccupations, vérifier les données de rendement (p. ex. les progrès vers l'atteinte des résultats souhaités) et corriger la situation, au besoin.

g) La publication des améliorations n'est pas astreinte à un calendrier. Des améliorations peuvent se produire aussi souvent que possible afin que le client d'affaires et les autres utilisateurs retirent le maximum d'avantages. En publiant fréquemment de petites mises à jour, l'équipe pourra avoir encore plus l'assurance que les modifications qu'elle apporte n'ont pas d'effet négatif sur le rendement du système ou sur l'atteinte de ses résultats.

6.3 Exigences de gestion du calendrier

a) L'entrepreneur doit gérer le calendrier du projet à toutes les étapes du cycle de vie du contrat et en assumer la responsabilité, car la réussite du projet dépend fortement d'un calendrier intégré et fiable qui définit le moment où les travaux auront lieu et la façon dont les activités du projet sont interdépendantes.

b) Le calendrier du projet de l'entrepreneur doit décrire une feuille de route avec les capacités opérationnelles obligatoires reposant sur la hiérarchisation des produits livrables communiquée par le client d'affaires et figurant dans le présent EDT.

c) L'entrepreneur doit utiliser ses propres paramètres pour mesurer les progrès et estimer l'effort restant. À la fin de chaque sprint, l'entrepreneur doit analyser les données de progression afin de déterminer si le niveau d'effort des tâches a été sous-estimé ou surestimé, ce qui permet une planification plus précise des sprints ultérieurs.

6.4 Cadre de planification et de contrôle

a) L'entrepreneur doit tenir à jour un cadre de planification et de contrôle pour la durée du contrat. Les produits livrables du contrat doivent être exécutés, livrés et mis à jour conformément au calendrier de livraison figurant dans le présent document et précisé dans le calendrier de projet proposé par l'entrepreneur.

6.5 Plan de gestion de projet

a) L'entrepreneur doit fournir un plan de gestion de projet, qui décrit les processus que l'entrepreneur utilisera afin de s'assurer que le contrat et la livraison de la solution sont exécutés conformément aux modalités du contrat, aux politiques gouvernementales établies et aux normes de l'industrie en matière de gestion des projets.

b) L'entrepreneur doit également décrire son plan de gestion des risques, en indiquant comment il compte déterminer, atténuer, gérer et signaler les risques pendant l'exécution du contrat.

c) L'entrepreneur doit également décrire son plan de gestion des problèmes, en fournissant des détails sur les processus et les procédures par lesquels les problèmes liés à l'exécution du contrat seront transmis à une autorité supérieure aux fins de décision et de résolution.

d) L'entrepreneur doit décrire son processus de gestion du changement afin de présenter son approche et ses procédures de traitement, d'autorisation et de gestion des changements eu égard aux exigences, à la portée, au calendrier et aux coûts pendant l'exécution du contrat.

e) L'entrepreneur doit utiliser des processus de gestion de la configuration afin d'aviser rapidement le Canada de toute interruption qui pourrait toucher la disponibilité et la performance des services, selon les exigences énoncées à la Section 3.18 – Paramètres de rendement et à la Section 3.15 – Disponibilité et rendement de la solution.

f) L'entrepreneur doit indiquer comment il abordera la mobilisation des intervenants et la communication. Cela comprend l'identification des intervenants, l'analyse des intervenants visant à déterminer leur influence et leur intérêt dans l'exécution du contrat, la définition d'approches destinées à mobiliser les intervenants, les rôles et les responsabilités pour le processus de mobilisation des intervenants.

g) L'entrepreneur peut décider du contenu et du format de ce produit livrable et du nombre d'artefacts (p. ex. diagrammes, vues, modèles et matrices) qu'il peut fournir. Les artefacts soumis doivent être clairs et concis, bien décrits et permettre au gouvernement du Canada de comprendre comment les exigences ont été satisfaites.

6.6 Ressources du projet

6.6.1 Gestionnaire principal de projet de l'entrepreneur

a) L'entrepreneur doit nommer un gestionnaire principal de projet (GPP) contractuel.

b) Le GPP doit assurer la gestion et la coordination quotidiennes du contrat et doit être le point de contact au sein de l'organisation de l'entrepreneur pour la livraison des biens et services associés au contrat.

c) Le GPP doit avoir une expérience antérieure en gestion de projets de GI/TI du gouvernement fédéral canadien d'une valeur de plus de 10,0 millions de dollars canadiens.

6.6.2 Ressources techniques

a) En plus du GPP et des ressources contractuelles de base, le Canada peut avoir besoin des services de plusieurs ressources pour fournir des services techniques et un soutien technique. Les services de ces ressources seront acquis au moyen des autorisations de tâches.

b) L'entrepreneur doit s'engager à rendre disponibles les ressources techniques voulues pour qu'elles puissent fournir ces services.

7. Produits livrables de la phase 2

7.1 Aperçu

a) L'entrepreneur doit fournir une solution entièrement fonctionnelle et doit prévoir et fournir un soutien continu, y compris :

i) gestion de projet;

ii) configurations de la conception du système;

iii) déploiement du système;

iv) documentation;

v) tests;

vi) support des usagers;

vii) offrir des consultations approfondies, selon la demande, au sujet des pratiques exemplaires et de l'efficacité des processus, et assurer une intégration réussie avec les processus, les procédures et l'environnement technologique existants du responsable technique;

viii) fournir la formation requise destinée aux utilisateurs avancés et aux experts en la matière et le matériel de formation, selon la demande;

ix) fournir un soutien pour veiller à ce que la GRC maximise à la fois la flexibilité et la rentabilité de la solution.

b) Pour assurer le succès de la mise en œuvre de la solution, le projet comprendra, au minimum, les produits livrables liés à la mise en œuvre mentionnés ci-dessous. Chaque produit livrable doit être créé par l'entrepreneur et doit être officiellement présenté au responsable technique aux fins d'examen et d'acceptation. Pour les jalons comportant plusieurs étapes, chaque étape doit contenir tous les produits livrables (sauf indication contraire).

c) L'entrepreneur doit utiliser les applications Microsoft Office approuvées par le gouvernement du Canada (Word, Excel, PowerPoint, Visio et Project) pour créer et mettre à jour les produits livrables. Tous les documents doivent être pleinement modifiables afin qu'ils puissent être mis à jour par le gouvernement du Canada. Si l'entrepreneur souhaite soumettre les documents sous un autre format électronique, la demande doit être expressément approuvée par le gouvernement du Canada.

d) La mise en œuvre de la phase 2 commence à la date à laquelle le gouvernement du Canada exerce son option de demander à l'entrepreneur de fournir la solution complète (travaux de phase 2) et doit prendre fin environ 17 mois suivant la date de l'exercice de cette option par le gouvernement du Canada.

7.2 Liste des produits livrables de la phase 2

a) L'entrepreneur doit fournir les produits livrables suivants :

i) Une **réunion de lancement de la phase 2** qui doit être prévue dans un délai d'une (1) semaine à compter de la date de l'exercice de l'option des travaux de la phase 2 par le Canada et qui doit :

(1) porter de façon générale sur l'approche et la méthodologie, le contrat, les relations de travail, les échéanciers, les risques et les enjeux touchant la phase 2;

(2) être présidée par l'autorité contractante de SPAC;

(3) inclure un ordre du jour et une présentation, le cas échéant, à fournir à l'autorité contractante dans un délai raisonnable avant la date de la réunion;

(4) inclure le procès-verbal de la réunion à fournir à l'autorité contractante pour approbation, avant distribution à toutes les autorités.

ii) Un **calendrier de la phase 2** qui doit inclure :

(1) la portée des travaux de la phase 2, y compris les jalons prévus, les produits livrables, les dépendances, les itérations / sprints basés sur les priorités des capacités opérationnelles (GCO de la SNC) à réaliser dans le cadre du présent Énoncé des travaux (EDT);

(2) le calendrier de mise en œuvre;

(3) sous réserve de l'approbation du responsable technique de la GRC, étant entendu que les détails du calendrier peuvent être modifiés au cours de la phase 2 si la GRC et l'entrepreneur décident ensemble que c'est dans l'intérêt du projet.

iii) Un **plan de gestion de projet** pour les travaux de la phase 2 (voir la Section 6.5 - Plan de gestion de projet), qui doit inclure, mais sans s'y limiter :

(1) Sommaire – Décrire à un niveau élevé les éléments clés du projet qui sont détaillés dans le plan de gestion de projet;

(2) Gouvernance du projet – Décrire la gouvernance du projet, y compris les rôles et responsabilités des principaux membres de l'équipe de projet;

(3) Méthodologie de développement – Décrire la méthodologie qui sera utilisée pour gérer le processus de développement et d'intégration de la solution logicielle;

(4) Méthodologie de gestion de projet – Décrire l'approche qui sera utilisée pour gérer le projet;

(5) Portée du projet – Il convient de définir la portée de la phase 2 ainsi que les principaux produits livrables. Les hypothèses du projet devraient également être incluses, afin de clarifier les zones d'ombre dans la portée du projet;

(6) Contraintes – Une liste de toutes les contraintes connues liées à l'exécution du projet;

(7) Dépendances – Une liste des dépendances connues du projet;

(8) Gestion des risques – Détailler le processus à employer dans le cadre du projet afin de gérer les risques;

(9) Gestion des problèmes – Définir le processus à utiliser pour gérer les problèmes relevés dans le cadre du projet;

(10) Gestion du changement – Décrire le processus de gestion du changement à utiliser dans le cadre du projet;

(11) Mobilisation des intervenants et communication.

iv) Des **rapports de progrès**, qui doivent :

(1) être fournis au responsable technique de la GRC deux fois par mois : le 15 et le dernier jour du mois;

(2) décrire les progrès de l'entrepreneur à l'égard des étapes clés du projet définies et approuvées dans le produit livrable du calendrier de la phase 2;

(3) établir les secteurs de risque, les décalages, le chemin critique du projet et les secteurs à problèmes;

(4) indiquer les problèmes nécessitant une atténuation, des décisions ou une résolution;

(5) comprendre un tableau de bord du projet pour la direction qui présente de façon graphique les éléments clés des différents paramètres (p. ex. portée, coût, calendrier, risques et problèmes) associés à l'exécution du contrat.

v) Des **réunions d'examen des progrès**, qui doivent :

(1) être tenues deux fois par mois;

(2) être présidées par l'autorité contractante de la GRC;

(3) respecter les lignes directrices gouvernementales sur la COVID-19 concernant le rassemblement et l'éloignement social;

(4) être menées conformément à l'ordre du jour des réunions d'examen des progrès (REP) qui doit être fourni par l'entrepreneur;

(5) comprendre un procès-verbal, qui doit contenir un compte rendu de décisions, les mesures à prendre et tout autre point de discussion abordé durant la REP. Ces procès-verbaux doivent être soumis au gouvernement du Canada trois (3) jours ouvrables après la REP;

(6) en plus des REP prévues, le gouvernement du Canada peut, à son entière discrétion, demander à l'entrepreneur d'être représenté dans le cadre de réunions extraordinaires, où il est possible d'aborder des questions sérieuses pour lesquelles on ne peut attendre jusqu'à la prochaine réunion d'examen des progrès.

vi) Un **plan de mise en œuvre de la solution** pour les travaux de la phase 2 qui doit inclure ce qui suit :

(1) L'entrepreneur doit démontrer que toutes les capacités techniques et opérationnelles ont été prises en compte dans le plan de mise en œuvre, étant entendu que la priorité et les spécificités des capacités individuelles seront déterminées en collaboration au cours de la phase 2 par la GRC et l'entrepreneur.

(2) Le plan de mise en œuvre doit comprendre au moins les éléments suivants :

a) une description de l'approche itérative et de la méthodologie que l'entrepreneur utilisera pour configurer, intégrer et lancer la solution, y compris la manière dont les défis liés à la COVID-19 seront relevés;

b) une description des étapes prévues pour le déploiement itératif (versions progressives), l'installation et la mise en œuvre pendant la durée du contrat;

c) un ensemble détaillé d'instructions étape par étape (c.-à-d. un manuel d'installation) clair, précis et suffisamment détaillé pour permettre au gouvernement du Canada d'installer les composantes applicables de la solution dans l'espace infonuagique Protégé B de la GRC;

d) une liste des licences d'infrastructures et de logiciels pour la solution;

e) une liste détaillée des ressources qui seront hébergées dans l'espace infonuagique protégé B de la GRC afin de fournir, d'exploiter et de faire évoluer la solution;

f) le modèle de données doit comprendre une corrélation entre les tailles (p. ex. unité de gestion des stocks [UGS]) dans un scénario évolutif;

g) une description technique de la méthode de conditionnement ou de distribution ou des archives d'installation pour chacun des composants d'infrastructure et des composants logiciels utilisés dans la solution. En voici des exemples hypothétiques : Images Docker, scripts Terraform, binaires Linux, WebArchives et logiciel Windows;

h) une description technique de toutes les technologies et services nécessaires pour développer, mettre en œuvre, exploiter et maintenir la solution. Exemples hypothétiques : Jenkins, Jira, apt-get, Trello, Git-Lab;

i) une description des outils et des processus de configuration et de contrôle de version qui seront mis en place pour gérer les déploiements itératifs;

j) une description du modèle de services infonuagiques de la solution décrivant comment la solution est déployée en ce qui concerne les modèles de services infonuagiques (IaaS ou PaaS privée dans un espace infonuagique de la GRC, SaaS ou PaaS public ou solution hybride).

(3) il revient à l'entrepreneur de décider du meilleur format et du nombre d'artefacts (p. ex. diagramme, vues, modèles, matrices) nécessaires. Les artefacts soumis doivent être clairs et concis, bien décrits et permettre au responsable technique de comprendre comment les exigences ont été satisfaites.

vii) Un **plan de gestion de la sécurité** qui doit décrire :

(1) les contrôles de sécurité qui seront mis en œuvre et dont on effectuera le suivi selon l'évaluation de sécurité de l'entrepreneur;

(2) les rôles et responsabilités de l'entrepreneur quant à la sécurité;

(3) le processus pour cerner et signaler les incidents de sécurité et pour y réagir;

(4) le renforcement de la sécurité des systèmes, y compris la gestion continue des correctifs.

viii) Un **plan de reprise après sinistre (PRS)**, qui doit documenter et décrire :

(1) une approche structurée quant à la façon dont la GRC peut rapidement reprendre le travail après un incident non prévu touchant la solution, y compris :

a) l'établissement de l'étendue ou de l'importance du traitement et des mesures nécessaires – la portée du rétablissement;

b) la collecte des documents pertinents quant à l'infrastructure du réseau;

c) l'établissement des menaces et des vulnérabilités les plus graves, ainsi que des actifs les plus critiques.

(2) les procédures pour mettre à jour le PRS et lancer une vérification à cet égard;

(3) les procédures pour aider la GRC à résoudre les pertes de données et à rétablir la fonctionnalité du système, afin que celui-ci puisse effectuer des tâches après un incident, même à un niveau minimal;

(4) consulter la Section 3.6 – Plan de reprise après sinistre du présent énoncé des travaux pour obtenir de plus amples détails.

ix) Un **plan de sauvegarde et de reprise** qui décrit au minimum :

(1) les procédures;

(2) les rôles et responsabilités;

(3) les processus de vérification et d'essai;

(4) les processus d'avis en cas d'erreur;

(5) les processus de restauration.

x) **Un plan de continuité de la technologie de l'information**

(1) Décrire au minimum les procédures d'invocation, les procédures d'évaluation et d'acheminement au palier supérieur, les rôles et responsabilités, les journaux d'incidents, les procédures de repli et les procédures de rétablissement des services jusqu'à la prestation normale des services.

xi) Une **architecture de système**

(1) décrit les composantes et les caractéristiques qui seront livrées par l'entrepreneur, avec un calendrier de l'intégration de ces composantes dans l'architecture de la solution;

(2) fournit l'architecture du système.

xii) Un **document de conception du système**

(1) voir la Section 3.5 – Documentation technique de la solution du présent énoncé des travaux pour plus de détails.

xiii) Un **plan de sécurité du système**

(1) conformément aux produits livrables décrits dans la Section 5 – Plan de sécurité du système du présent énoncé des travaux.

xiv) Une **évaluation de sécurité et autorisation**

(1) conformément aux détails fournis dans la Section 3.5 – Documentation technique de la solution du présent énoncé des travaux.

xv) Un **modèle des données réelles**

(1) fournit un modèle des données réelles du dépôt de la solution.

xvi) Un **plan de cycle de vie de l'information**

(1) décrire le cycle de vie complet de la gestion des données (de la collecte à l'élimination), y compris les processus mis en place pour gérer les données qui ont atteint les délais de conservation.

xvii) Un **plan de formation**

(1) décrire comment l'entrepreneur prévoit offrir les ressources initiales et mises à jour de formation, dans les deux langues (anglais et français);

(2) voir la Section 3.10.1 – Plan de formation du présent énoncé des travaux pour plus de détails.

xviii) Des **documents de formation**

(1) doivent être fournis en anglais et en français et comprendre des copies électroniques des manuels d'utilisation, des manuels techniques et des autres documents à l'intention des utilisateurs dont on a besoin pour apprendre comment utiliser la solution et l'entretenir;

(2) voir la Section 3.10.2 – Matériel de formation du présent énoncé des travaux pour plus de détails.

xix) **Prestation de la formation**

(1) La formation doit être fournie en anglais et en français;

(2) voir la Section 3.10.3 – Prestation de la formation du présent énoncé des travaux pour plus de détails.

xx) Un **plan d'essais d'acceptation de la solution**, qui doit comprendre :

(1) une description de la planification et des essais qui seront entrepris pour la solution prototype;

(2) une description des procédures générales d'acceptation pour la planification, la préparation et l'achèvement des essais;

(3) voir la Section 3.7 – Plan d'essais d'acceptation de la solution du présent énoncé des travaux pour plus de détails.

xxi) Un **rapport d'essais d'acceptation de la solution**, qui doit comprendre :

(1) les résultats des essais d'acceptation de la solution réalisés conformément au plan d'essais d'acceptation de la solution;

(2) la confirmation que la solution a réussi tous les essais d'acceptation requis et satisfait aux exigences énoncées dans le contrat ou que la solution a échoué aux essais d'acceptation avec les raisons de l'échec;

(3) voir la Section 3.8 – Rapport d'essai d'acceptation de la solution du présent énoncé des travaux pour plus de détails.

xxii) **SNC et documentation**

(1) inclure le lancement de versions successives de la solution jusqu'à ce que la pleine capacité opérationnelle soit atteinte;

(2) voir la Section 3.4 – Solution logicielle et documentation du présent énoncé des travaux pour plus de détails.

xxiii) Un **plan de transition**

(1) conformément aux détails fournis dans la Section 3.12 – Plan de transition du présent énoncé des travaux.

xxiv) Un **plan de transition de sortie**

(1) conformément aux détails fournis dans la Section 3.13 – Plan de transition de sortie du présent énoncé des travaux.

xxv) **Services professionnels et services de formation**

(1) doivent être fournis, au besoin, pour la mise en œuvre de la solution, la migration des données et d'autres services spécialisés.

xxvi) Un **rapport de fin de projet** pour marquer l'achèvement du projet. Le rapport doit permettre :

(1) d'évaluer le rendement et les résultats du projet, de cerner les leçons apprises et de confirmer que les activités essentielles prévues dans le contrat et les autres activités d'achèvement du projet ont été réalisées;

(2) d'achever le transfert des actifs, des produits livrables et de toutes les fonctions administratives continues à l'organisme de services de la GRC;

(3) il revient à l'entrepreneur de décider du meilleur format et du nombre d'artefacts (p. ex. diagramme, vues, modèles, matrices) qui sont nécessaires. Les artefacts soumis doivent être clairs et concis, bien décrits et permettre au responsable technique de comprendre comment les exigences ont été satisfaites.

7.3 Calendrier des produits livrables de la phase 2

a) Le tableau suivant contient les produits livrables pour la phase 2 au titre du contrat ainsi que les dates de livraison. Les produits livrables doivent être présentés au responsable technique selon le format précisé, à la date de livraison convenue. Tous les délais énoncés dans le tableau des produits livrables sont en jours ouvrables.

Tableau 7-1 : Liste et calendrier des produits livrables au titre du contrat

Nº	Description	Date de livraison
1.	Réunion de lancement de la phase 2	1 semaine à compter de la date d'exercice de l'option de travaux de la phase 2
2.	Calendrier de la phase 2; copie numérique remise au responsable technique du client	2 semaines à compter de la date d'exercice de l'option de travaux de la phase 2
3.	Plan de gestion de projet; copie numérique remise au responsable technique du client	3 semaines à compter de la date d'exercice de l'option de travaux de la phase 2
4.	Rapports de progrès; copie numérique remise au responsable technique du client	Deux fois par mois à compter de la date d'exercice de l'option de travaux de la phase 2
5.	Réunions d'examen des progrès	Deux fois par mois à compter de la date d'exercice de l'option de travaux de la phase 2
6.	Plan de mise en œuvre de la solution finale; copie numérique remise au responsable technique du client	4 semaines à compter de la date d'exercice de l'option de travaux de la phase 2
7.	Plan de gestion de la sécurité; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
8.	Plan de reprise après sinistre; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
9.	Plan de sauvegarde et de reprise; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
10.	Plan de continuité de la technologie de l'information; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
11.	Architecture du système; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2

Tableau 7-1 : Liste et calendrier des produits livrables au titre du contrat

Nº	Description	Date de livraison
12.	Document de conception du système; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
13.	Plan de sécurité du système; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
14.	Une évaluation et autorisation de sécurité	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
15.	Modèle physique des données; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
16.	Plan de continuité de la technologie de l'information; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
17.	Plan de formation; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
18.	Document de formation; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
19.	Prestation de la formation	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
20.	Plan d'essais d'acceptation de la solution; copie numérique remise au responsable technique du client	5 semaines à compter de la date d'exercice de l'option de travaux de la phase 2
21.	Rapport d'essais d'acceptation de la solution; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
22.	SNC et documentation – plusieurs versions	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2

Tableau 7-1 : Liste et calendrier des produits livrables au titre du contrat

Nº	Description	Date de livraison
23.	Plan de transition; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
24.	Plan de transition de sortie	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2
25.	Des services professionnels et services de formation	Sur demande
26.	Un rapport de fin de projet; copie numérique remise au responsable technique du client	Conformément au calendrier de l'entrepreneur pour les produits livrables de la phase 2

8. Documents de référence

a) *Loi sur l'accès à l'information* : https://laws-lois.justice.gc.ca/fra/lois/a-1/

b) Centre canadien pour la cybersécurité, Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) : https://cyber.gc.ca/fr/orientation/exigences-de-base-en-matiere-de-securite-pour-les-zones-de-securite-de-reseau-au-sein

c) Centre canadien pour la cybersécurité, Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques : https://cyber.gc.ca/sites/default/files/publications/itsm.50.100-fr.pdf

d) Centre canadien pour la cybersécurité, Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROGÉGÉ A, et PROTÉGÉ B (ITSP.40.111) : https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b

e) Centre canadien pour la cybersécurité, Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) : https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062

f) Centre canadien pour la cybersécurité, Nettoyage des supports de TI (ITSP.40.006) : https://www.cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006

g) Centre canadien pour la cybersécurité, Considérations de conception relatives au positionnement des services dans les zones (ITSG-38) : https://www.cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones

h) Centre canadien pour la cybersécurité, Correction des systèmes d'exploitation et des applications - Bulletin de sécurité des TI à l'intention du gouvernement du Canada (ITSB-96) : https://cyber.gc.ca/fr/orientation/correction-des-systemes-dexploitation-et-des-applications-bulletin-de-securite-des-ti

i) Centre canadien pour la cybersécurité, Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3) : https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de

j) Centre de sécurité des télécommunications, Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information : https://www.cse-cst.gc.ca/fr/node/2454/html/28582

k) Normes d'architecture d'entreprise du gouvernement du Canada (en anglais seulement) : https://wiki.gccollab.ca/Government_of_Canada_Architectural_Standards

l) Catalogue des services de courtage infonuagiques GC : https://cloud-broker.canada.ca/s/pbmmcatalogpage?language=fr_CA

m) Normes numériques du gouvernement du Canada : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/normes-numeriques-gouvernement-canada.html

n) Lignes directrices du gouvernement du Canada sur l'utilisation responsable de l'intelligence artificielle (IA) : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/utilisation-responsable-ai.html

o) Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada – Avis de mise en œuvre de la *Politique sur la technologie de l'information* (AMPTI) : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/avis-mise-oeuvre-politique/utilisation-securisee-stockage-donnees-portatifs-gouvernement.html

p) Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html

q) Normes du gouvernement du Canada sur les API : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html

r) Organisation internationale de normalisation (ISO), Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015) : https://www.iso.org/standard/43757.html

s) Organisation internationale de normalisation (ISO), Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2019) : https://www.iso.org/standard/76559.html

t) Organisation internationale de normalisation (ISO), Information technology – Security techniques – Information technology — Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013) : https://www.iso.org/standard/54534.html

u) Conseils en matière de sécurité des technologies de l'information – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) : https://cyber.gc.ca/fr/orientation/annexe-3a-catalogue-des-controles-de-securite-itsg-33

v) *Loi sur la Bibliothèque et les Archives du Canada* : https://laws-lois.justice.gc.ca/fra/lois/L-7.7/index.html

w) Bibliothèque et Archives Canada, Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires : https://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formats-fichier-transferers-ressources-documentaires.aspx

x) National Institute of Standards ND Technology (NIST), Cryptographic Algorithm Validation Program: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

y) National Institute of Standards ND Technology (NIST), Security Requirements for Cryptographic Modules (FIPS 140-2): https://csrc.nist.gov/publications/detail/fips/140/2/final

z) *Loi sur les langues officielles* : https://laws-lois.justice.gc.ca/fra/lois/o-3.01/

aa) *Loi sur la protection des renseignements personnels* : https://laws-lois.justice.gc.ca/fra/lois/P-21/index.html

bb) Services publics et Approvisionnement Canada, Les documents pour le transfert des fichiers sécurisé : https://sftweb.pwgsc.gc.ca/sft-html/Documents_f.html

cc) Services publics et Approvisionnement Canada, L'informatique en nuage – Véhicule d'approvisionnement « les logiciels en tant que service » : https://www.tpsgc-pwgsc.gc.ca/app-acq/cral-sarc/saas-fra.html

dd) Profil de contrôle de sécurité ministérielle de la GRC : Disponible sur demande de l'autorité contractante

ee) GRC, G1-009 – Transport et transmission de renseignements protégés ou classifiés : https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-fra.htm

ff) GRC, G1-025 – Protection, détection et intervention : https://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-025-fra.htm

gg) Guide des clauses et conditions uniformisées d'achat (CCUA) 2003 : https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat

hh) Secrétariat du Conseil du Trésor du Canada, Évaluation de l'incidence algorithmique (EIA) : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/utilisation-responsable-ai/evaluation-incidence-algorithmique.html

ii) Secrétariat du Conseil du Trésor, Chapitre 6 – Manipulation et protection de renseignements et de biens : https://www.tpsgc-pwgsc.gc.ca/esc-src/msc-csm/chap6-fra.html

jj) Secrétariat du Conseil du Trésor, Directive sur la prise de décision automatisée : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592

kk) Secrétariat du Conseil du Trésor, Directive sur la gestion de la sécurité : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611

ll) Secrétariat du Conseil du Trésor, Directive sur la gestion de projets et programmes : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32594

mm) Secrétariat du Conseil du Trésor, Niveaux de sécurité : https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html

nn) Secrétariat du Conseil du Trésor, Projet d'activation et de défense du nuage sécurisé : https://wiki.gccollab.ca/L%27infocentre_de_l%27infonuagique

oo) Norme du gouvernement du Canada sur les métadonnées : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18909

pp) Secrétariat du Conseil du Trésor, Norme sur le filtrage de sécurité : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115

qq) Secrétariat du Conseil du Trésor, Norme sur l'accessibilité des sites Web : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601

rr) Normes d’accessibilité WCAG 2.0 A : https://www.w3.org/Translations/WCAG20-fr/ et https://www.w3.org/WAI/standards-guidelines/fr

Appendice A – Évaluation des capacités et de la convivialité (ECC)

A.1 Objet

a) Le présent document décrit le processus d'évaluation des capacités, de la convivialité, de l'accessibilité et de l'innovation.

A.2 Directives

a) L'entrepreneur doit élaborer et présenter une solution prototype infonuagique qui sera évaluée par le gouvernement du Canada.

b) L'entrepreneur doit fournir au gouvernement du Canada, aux fins de l'ECC, un soutien quant à la solution prototype ainsi qu'un accès non restreint à celle-ci, y compris l'octroi de tous les droits d'utilisation de la solution prototype, les documents relatifs au logiciel, la garantie, l'hébergement, le stockage, la maintenance et le soutien (à l'exception de la formation), les renonciations, les ententes de non-divulgation, les scripts de scénarios de test pour l'ECC et les autres versions.

c) Le gouvernement du Canada doit avoir accès à l'ECC et disposer d'un droit d'accès pour cent (100) utilisateurs afin de mettre à l'essai la solution prototype et d'effectuer l'ECC.

d) L'entrepreneur doit fournir au gouvernement du Canada toutes les instructions nécessaires pour utiliser la solution prototype et effectuer l'ECC.

e) Le gouvernement du Canada fournira à l'entrepreneur des échantillons de données qui doivent être utilisés pour valider les cas d'utilisation du prototype.

A.3 Sélection de la solution prototype de l'entrepreneur

a) Les produits livrables de la solution prototype aux fins de l'ECC fournis au titre du contrat seront évalués par le gouvernement du Canada en fonction des critères détaillés dans l'appendice A – Évaluation des capacités et de la convivialité de l'annexe A – Énoncé des travaux.

b) L'ECC comprendra quatre (4) différentes catégories d'évaluation. Les voici :

   i) Partie un : Évaluation des capacités au moyen de scénarios : sert à mesurer la capacité fonctionnelle de la solution prototype à effectuer des tâches et à répondre aux exigences précisées dans l'annexe A – Énoncé des travaux.

   ii) Partie deux : Évaluation selon l'échelle de convivialité du système : sert à mesurer la facilité d'utilisation par les utilisateurs de la solution prototype, y compris l'expérience et la satisfaction générales de l'utilisateur relativement à la solution prototype.

iii) Partie trois : Évaluation selon l'échelle de convivialité des mesures d'accessibilité : sert à mesurer la facilité d'utilisation de la solution prototype au moyen des différentes technologies d'aide pour répondre aux besoins en matière d'accessibilité et d'accommodement, conformément à la Norme sur l'accessibilité des sites Web du gouvernement du Canada[1], y compris pour évaluer l'expérience et la satisfaction générales des utilisateurs à l'égard de la solution prototype.

iv) Partie quatre : Évaluation de l'innovation : sert à mesurer le degré d'innovation dont fait preuve l'entrepreneur.

c) Le tableau ci-dessous fournit le nombre maximum de points qui peuvent être obtenus dans chaque catégorie :

Tableau A-1 : Sommaire des notes de l'ECC

Catégorie de l'ECC	Note maximale
Partie un : Évaluation des capacités au moyen de scénarios	700
Partie deux : Évaluation selon l'échelle de convivialité du système	85
Partie trois : Évaluation selon l'échelle de convivialité des mesures d'accessibilité	50
Partie quatre : Innovation	140
Total des points	**975**

d) La somme des points pour chaque catégorie d'évaluation sera calculée conformément aux critères d'évaluation et au nombre maximal de points précisé pour chaque catégorie mentionnée à l'appendice A. On établira la note globale d'évaluation pour la solution prototype en additionnant la note obtenue dans chacune des quatre catégories de l'ECC.

[1] Pour obtenir plus de renseignements concernant la Norme sur l'accessibilité des sites Web du Canada, consultez la page https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601

e) Au besoin, le Canada peut effectuer, à sa seule discrétion; un essai de prototype sur plateforme (POP) en utilisant la solution prototype proposée par l'entrepreneur ayant obtenu la meilleure note (identifié après l'évaluation des capacités et de la convivialité (ECC) afin de confirmer qu'elle fonctionnera comme décrite dans le modèle de services infonuagiques de la solution de l'entrepreneur. Le Canada documentera les résultats du test de prototype sur plateforme. Si le gouvernement du Canada établit que la solution proposée ne répond pas aux exigences relatives au test de prototype sur plateforme, l'entrepreneur sera considéré comme ayant échoué au test et sera rejeté. Lorsque l'entrepreneur ayant obtenu la meilleure note échoue au test de prototype sur plateforme, le gouvernement du Canada peut, à sa seule discrétion, soumettre la solution proposée par l'entrepreneur s'étant classé au deuxième rang (désigné après l'ECC) au test.

f) Lorsque l'entrepreneur réussit toutes les évaluations, le gouvernement du Canada, à son entière discrétion, se prévaudra de son option irrévocable de choisir l'entrepreneur pour qu'il exécute l'ensemble ou une partie des travaux de la phase 2 au titre de la section Phase 2 – Solution complète de l'annexe A – Énoncé des travaux. Le gouvernement du Canada peut également, à sa discrétion, se prévaloir de son option irrévocable de choisir d'autres entrepreneurs qui ont participé à l'ECC afin de leur confier l'ensemble ou une partie des travaux s'il est établi que cela permettrait de mieux répondre aux besoins du gouvernement du Canada.

Tableau A-2 : Évaluation des capacités au moyen de scénarios – Légende

ÉVALUATION DES CAPACITÉS ET DE LA CONVIVIALITÉ – PARTIE UN : ÉVALUATION DE LA CAPACITÉ AU MOYEN DE SCÉNARIOS		
Résultat	**Note**	**Description**
Non établi	0 point	La solution prototype possède 30 % ou moins des fonctionnalités requises au chapitre de la capacité.
Partiellement établi	3 points	La solution prototype possède plus de 30 %, mais moins de 60 % des fonctionnalités requises au chapitre de la capacité.
Établi en grande partie	6 points	La solution prototype possède 60 % ou plus, mais moins de 90 % des fonctionnalités requises au chapitre de la capacité.
Pleinement établi	10 points	La solution prototype possède 90 % ou plus des fonctionnalités requises au chapitre de la capacité.

Tableau A-3 : ECC – Scénario 1 – Demande de service d'un partenaire

SCÉNARIO 1 – Demande de service d'un partenaire **Thèmes du scénario :** Gestion de l'identité, gestion des cas, répertoire CRM, recherche, notification, transfert sécurisé de l'information, Portail des partenaires et des policiers
Récit de l'utilisateur Un nouveau partenaire transmet un rapport de cyberactivité (RCA) au moyen d'un courriel sécurisé. Le RCA fournit une liste de routeurs et d'adresses IP au Canada qui pourraient avoir été compromis par des auteurs malveillants qui cherchent à faire du minage de cryptomonnaie malveillant et à obtenir un accès non autorisé à un réseau. Intrant : Le GNCC reçoit le RCA au moyen d'un courriel sécurisé. Le GNCC enrichira la demande et déterminera toute corrélation avec des renseignements existants provenant du GNCC ou de sources externes. Toute l'information détaillée sur les adresses IP et les routeurs figure dans une pièce jointe en format Excel (p. ex. CSV) envoyée avec le courriel (entités visées par un indicateur de compromission = 1,000). Avant la réception de ce RCA, un autre partenaire a créé une « liste de surveillance » à l'aide du P3 qui contient certaines des entités (p. ex. adresses IP d'intérêt) figurant dans le RCA.
La solution prototype devrait permettre au GNCC :
• De recevoir automatiquement des notifications par courriel lorsqu'une nouvelle demande de service est reçue par courriel. • De se connecter de façon sécuritaire à la solution. • D'accéder à la liste des travaux en attente propre à un utilisateur pour voir les demandes qui sont automatiquement intégrées et stockées. • De visualiser les données structurées et non structurées qui ont été automatiquement comparées aux données internes et externes. • De modifier et de valider l'information reçue dans la demande ou les résultats de la recherche. • D'assigner la demande à un autre membre du groupe ou de demander à d'autres groupes que le GNCC d'enrichir la demande. • De déterminer et de produire la trousse de renseignements qui sera renvoyée à l'entité ayant présenté la demande au moyen d'un courriel sécurisé. • D'ajouter l'entité ayant présenté la demande au répertoire des partenaires. • De fermer la demande.
La solution prototype devrait permettre au partenaire :

- De se connecter de façon sécuritaire au P3.
- De créer une liste de surveillance.
- De recevoir automatiquement des notifications par courriel lorsqu'une corrélation est établie avec une information figurant dans la liste de surveillance.
- De recevoir des résultats sécurisés du GNCC sous la forme d'un rapport.

Scénario 1 – Grille de notation

N° de l'indicateur		Indicateurs	Non établi (0)	Partiellement établi (3)	Établi en grande partie (6)	Pleinement établi (10)
La solution prototype devrait fournir la fonctionnalité suivante :						
Capacité	**1**	Intégrer automatiquement les données contenues dans un courriel sécurisé, analyser et valider le contenu du courriel et tout indicateur de compromission et permettre à l'utilisateur d'ajouter le nouveau partenaire.	☐	☐	☐	☐
	2	Intégrer automatiquement les données de la pièce jointe Excel, analyser, cataloguer et valider tous les indicateurs de compromission.	☐	☐	☐	☐
	3	Hacher automatiquement le courriel et la pièce jointe et stocker l'algorithme de hachage.	☐	☐	☐	☐
	4	Effectuer une recherche automatique dans les sources internes et externes structurées et non structurées (p. ex. MISP) et faire correspondre les données.	☐	☐	☐	☐
	5	Lier la demande de service aux demandes antérieures dans la solution.	☐	☐	☐	☐
	6	Permettre à l'utilisateur du GNCC de se connecter en toute sécurité pour voir le billet et les liens.	☐	☐	☐	☐
	7	Établir une période de rétention de l'information ainsi que les protocoles de manipulation (p. ex. TLP) applicables.	☐	☐	☐	☐

	8	Envoyer automatiquement un courriel sécurisé à un partenaire qui a mis en place une « liste de surveillance » quant à ces indicateurs de compromission et lui permettre de voir les détails des correspondances avec sa « liste de surveillance » à partir de son compte du P3.	☐	☐	☐	☐
	9	Permettre à l'utilisateur du GNCC de voir, d'examiner et de modifier le contenu de la demande.	☐	☐	☐	☐
	10	Permettre à l'utilisateur du GNCC d'importer des coordonnées dans le répertoire des partenaires.	☐	☐	☐	☐
	11	Permettre à l'utilisateur du GNCC d'attribuer la demande à un autre utilisateur à des fins d'analyse approfondie.	☐	☐	☐	☐
	12	Permettre à un deuxième utilisateur du GNCC de voir la demande dans sa liste des travaux.	☐	☐	☐	☐
	13	Permettre à l'utilisateur du GNCC de choisir quelles données rassembler afin de créer un rapport.	☐	☐	☐	☐
	14	Permettre à l'utilisateur du GNCC de hacher et de chiffrer le rapport et de le communiquer par courriel à l'auteur de la demande.	☐	☐	☐	☐
	15	Permettre à l'utilisateur autorisé du GNCC de fermer la demande de service.	☐	☐	☐	☐
Note pour le scénario 1 :			**/150**			

Tableau A-4 : ECC – Scénario 2 – Municipalité touchée par un rançongiciel – Coordination et assistance

SCÉNARIO 2 – Municipalité touchée par un rançongiciel – Coordination et assistance **Thèmes du scénario :** Gestion de l'identité, gestion des cas, Portail des partenaires et des policiers, notifications, analyses des données, maintien des règles opérationnelles et des listes de surveillance, enrichissement automatique, gestion de l'information, clavardage, applications de publication de documents et de productivité, intégration.
Récit de l'utilisateur Le 21 mars 2020, l'infrastructure de technologie de l'information (TI) du ministère des Transports de Springson (MTS) a été infectée par un rançongiciel. Le MTS communique avec le service de police compétent. Au total, environ 3 000 systèmes sont touchés, dont 400 serveurs et l'ensemble des bases de données et des applications du MTS. Ces systèmes traitent des transactions d'une valeur d'environ 50 M$ chaque mois. Le service de police compétent signale l'incident au GNCC à l'aide du P3 et transmet par la suite des indicateurs de compromission. Vu la gravité de l'incident, la solution fixe un degré élevé de gravité et de priorité pour le GNCC. Celui-ci démarre une séance de clavardage de groupe en direct et crée un projet pour faciliter et coordonner les mesures et communiquer l'information aux partenaires policiers. Au départ, les efforts de mise en commun des renseignements se font du GNCC au partenaire, mais on inclut rapidement d'autres groupes qui pourraient avoir un rôle à jouer relativement à l'attaque et à l'enquête. Une demande d'information est envoyée aux partenaires par l'entremise du P3. Après que la demande a été diffusée aux partenaires, deux partenaires supplémentaires renvoient des renseignements au GNCC par l'entremise du P3 concernant le même rançongiciel, y compris les conséquences que celui-ci a eues dans leur territoire. Cela comprend un rapport (PDF) contenant de l'information à l'égard d'un acteur étranger soupçonné d'être lié au rançongiciel ainsi qu'une possible adresse courriel.
La solution prototype devrait permettre au GNCC :
• De recevoir une demande par l'entremise du Portail des partenaires et des policiers. • De trier, d'analyser et d'évaluer la demande en matière de cybercriminalité, ainsi que de faire correspondre les données. • D'utiliser les règles opérationnelles d'établissement des priorités pour aviser la Section de la coordination opérationnelle en fonction des attributs de la demande. • D'informer les partenaires de l'incident (l'équipe fédérale d'application de la loi dans le cyberespace, l'équipe provinciale d'application de la loi dans le cyberespace, le Groupe d'action mixte international sur la cybercriminalité et un partenaire canadien qui n'est pas issu du secteur de l'application de la loi). • De clavarder en direct avec tous les partenaires concernés – informer toutes les parties concernées de l'incident et du statut, discuter des prochaines étapes, mentionner comment le GNCC peut faciliter la prise de mesures et fournir son aide. • De créer et de gérer un projet.

- De transmettre une demande d'information à des partenaires choisis – demander aux partenaires s'ils ont de l'information concernant le rançongiciel.
- De classer la demande aux fins de la recherche de renseignements par le GNCC afin d'aider le service de police compétent.
- D'envoyer la trousse de renseignements aux partenaires.

La solution prototype devrait permettre au partenaire :

- De se connecter en toute sécurité au P3.
- De créer et de présenter une demande et de communiquer les indicateurs de compromission au moyen du P3.
- De participer à une séance de clavardage de groupe en direct par l'entremise du P3 avec le GNCC et d'autres partenaires du P3.
- De recevoir une notification par courriel relativement à une demande d'information.
- D'accéder à la demande d'information dans le P3.
- De répondre à la demande d'information.

Scénario 2 – Grille de notation

	N° de l'indicateur	Indicateurs	Non établi (0)	Partiellement établi (3)	Établi en grande partie (6)	Pleinement établi (10)
Capacités	1	Permettre à l'utilisateur du P3 de soumettre un incident de cybercriminalité et de demander de l'aide.	☐	☐	☐	☐
	2	Trier et analyser automatiquement l'information sur la cybercriminalité, y compris les indicateurs de compromission, et trouver automatiquement les correspondances.	☐	☐	☐	☐
	3	Déterminer et afficher le degré de gravité et de priorité à l'aide de la matrice de gravité et des règles d'établissement des priorités.	☐	☐	☐	☐
	4	Envoyer la demande au groupe de coordination opérationnelle pour qu'elle soit ajoutée à sa liste des travaux.	☐	☐	☐	☐

	5	Permettre à l'utilisateur du GNCC de lancer une séance de clavardage en direct avec les partenaires concernés et d'inviter des partenaires policiers à se joindre à la séance.	☐	☐	☐	☐
	6	Permettre aux organismes concernés du P3 de participer à la séance de clavardage en direct.	☐	☐	☐	☐
	7	Permettre à l'utilisateur du GNCC de créer un projet et de charger le groupe responsable du renseignement au sein du GNCC de mettre au point une trousse de renseignements.	☐	☐	☐	☐
	8	Permettre à l'utilisateur du GNCC d'envoyer concernés une demande d'information aux partenaires par le truchement du P3 en vue de leur demander s'ils ont des renseignements sur le rançongiciel.	☐	☐	☐	☐
	9	Permettre à l'utilisateur du P3 de voir le courriel de notification et d'ouvrir le P3 pour consulter les détails de la demande d'information quant à l'incident relatif au rançongiciel.	☐	☐	☐	☐
	10	Permettre aux partenaires du P3 de répondre à l'aide du P3 soit en fournissant des renseignements supplémentaires qui sont vérifiés par le GNCC et ajoutés au projet, soit en précisant qu'ils n'ont pas d'information à fournir.	☐	☐	☐	☐
	11	Permettre à l'utilisateur du GNCC de créer et d'envoyer une trousse de renseignements contenant tous les détails liés au rançongiciel aux partenaires concernés.	☐	☐	☐	☐
	12	Permettre à l'utilisateur du GNCC de fermer la demande de service.	☐	☐	☐	☐
Note pour le scénario 2 :			**/120**			

Tableau A-5 : ECC – Scénario 3 – Demande de partenaires concernant des conseils et une orientation en matière numérique

SCÉNARIO 3 – Demande de partenaires concernant des conseils et une orientation en matière numérique **Thèmes du scénario :** Gestion de l'identité, gestion des cas, analyse, répertoire CRM, recherche, notification, outils (reconnaissance optique de caractères, transcription, traduction), transfert sécurisé de l'information, intégration
Récit de l'utilisateur On reçoit une demande de conseils et de directives numériques d'un partenaire par l'entremise du Portail des partenaires et des policiers. La demande comprend : • Une image montrant un échange de courriels dans une langue qu'on croit être le russe; • Un fichier audio d'une conversation en anglais (1 à 2 minutes), en lien avec la cybercriminalité, entre plusieurs personnes. Comme ce partenaire n'a pas accès à des services numériques avancés, il utilise le P3 pour envoyer une demande d'aide au GNCC afin de faire traduire cet échange de courriels vers l'anglais et d'obtenir toute information connexe relativement au contenu des fichiers reçus ou de la conversation.
La solution prototype devrait permettre au GNCC :
• De recevoir une demande par l'entremise du Portail des partenaires et des policiers. • De trier, d'analyser et d'évaluer la demande et de faire correspondre les données. • D'utiliser les règles opérationnelles relatives au flux des travaux pour aviser la Section des conseils et de l'orientation techniques en fonction des attributs de la demande en matière de cybercriminalité. • D'examiner la demande. • D'accéder à des services de traduction, de transcription et de reconnaissance optique des caractères. • De rassembler les résultats. • Sur demande, d'envoyer au partenaire policier une trousse de divulgation à des fins judiciaires décrivant les tâches effectuées par le système et les mesures prises par le personnel du GNCC relativement à la demande originale transmise par le service de police compétent (y compris les fichiers de données présentés et enrichis). • De fermer la demande.
La solution prototype devrait permettre au partenaire de la police :

- De se connecter en toute sécurité au P3.
- De créer et d'envoyer une demande au moyen du P3, à laquelle des fichiers audio et des images peuvent être joints.
- De recevoir une notification par courriel lorsque la trousse de renseignements est disponible sur le P3 et d'accéder à la trousse de renseignements préparée par la Section des conseils et de l'orientation techniques.
- De recevoir des résultats sécurisés sous la forme d'une trousse de renseignements (de divulgation) du GNCC.

Scénario 3 – Grille de notation

	N° de l'indicateur	Indicateurs	Non établi (0)	Partiellement établi (3)	Établi en grande partie (6)	Pleinement établi (10)
Capacités	1	Permettre à l'utilisateur du P3 de présenter une demande d'aide en matière de cybercriminalité.	☐	☐	☐	☐
	2	Trier automatiquement la demande en matière de cybercriminalité.	☐	☐	☐	☐
	3	Établir au moyen des règles opérationnelles relatives au flux des travaux qu'il s'agit d'une demande de conseils et de directives numériques.	☐	☐	☐	☐
	4	En fonction des règles opérationnelles, attribuer automatiquement le billet à la Section des conseils et de l'orientation techniques du GNCC aux fins de traitement.	☐	☐	☐	☐
	5	Permettre à l'utilisateur du GNCC de voir la demande.	☐	☐	☐	☐
	6	Permettre à l'utilisateur du GNCC d'examiner la conversion de l'image en texte et d'apporter les changements nécessaires.	☐	☐	☐	☐
	7	Permettre à l'utilisateur du GNCC de traduire le texte généré vers l'anglais.	☐	☐	☐	☐
	8	Permettre à l'utilisateur du GNCC de convertir le fichier audio en texte.	☐	☐	☐	☐

	9	Analyser automatiquement l'information en matière de cybercriminalité, y compris les indicateurs de compromission, et trouver automatiquement les correspondances.	☐	☐	☐	☐
	10	Permettre à l'utilisateur du GNCC de voir les résultats suivants du traitement : • les langues que l'image et les fichiers contenaient; • l'image originale; • le texte extrait de l'image dans la langue originale; • la traduction du texte extrait en anglais; • le texte extrait du fichier audio, ce qui comprend la distinction entre les différents locuteurs dans le fichier audio (répartition du discours entre les locuteurs).	☐	☐	☐	☐
	11	Permettre à l'utilisateur du GNCC d'écouter le fichier audio original.	☐	☐	☐	☐
	12	Permettre à l'utilisateur du GNCC de préparer une réponse sous la forme d'une trousse de divulgation qui comprend toute nouvelle donnée, correspondance, analyse et conclusion.	☐	☐	☐	☐
	13	Permettre à l'utilisateur du GNCC de rendre l'information accessible au partenaire par l'entremise du P3.	☐	☐	☐	☐
	14	Permettre à l'utilisateur du GNCC d'aviser le partenaire policier au moyen d'un courriel sécurisé du fait que sa trousse de renseignements est prête.	☐	☐	☐	☐
	15	Permettre à l'utilisateur du P3 d'accéder à la trousse de renseignements dans le P3.	☐	☐	☐	☐
	16	Permettre à l'utilisateur du GNCC de fermer la demande.	☐	☐	☐	☐
Note pour le scénario 3 :			**/160**			

Tableau A-6 : ECC – Scénario 4 – Analytique

SCÉNARIO 4 – Analytique **Thèmes du scénario :** Gestion de l'identité, gestion des cas, recherche, tableau de bord, configuration, répertoire, notifications, analyse de données, enrichissement, transfert sécurisé de renseignements, intégration avec des applications de publication de documents et de productivité.
Récit de l'utilisateur Lien avec les scénarios 2 et 3 – Analytique Le GNCC a traité l'incident relatif au rançongiciel décrit dans le scénario 2 et, après la traduction des données du scénario 3, un lien est établi avec d'autres sources d'information, y compris en raison d'un indicateur de présence sur une « liste de surveillance » précédemment ajouté dans le système par deux autres services de police canadiens. Un utilisateur du GNCC interroge la solution, laquelle lance simultanément des recherches dans plusieurs sources et affiche tous les résultats. Ces recherches comprennent une recherche « approximative » dans diverses sources internes et externes, et des correspondances sont relevées avec différents types de renseignements, lesquelles établissent un lien entre ces deux incidents et d'autres renseignements. Les recherches sont effectuées par le GNCC et le partenaire. Le GNCC reçoit un résultat de CORRESPONDANCE SANS INTERVENTION, puisque certaines des données avaient précédemment été étiquetées pour l'envoi d'une notification de correspondance sans intervention. Des correspondances sont notamment relevées quant à une adresse IP, à une adresse courriel, à un sobriquet, des noms et à une adresse bitcoin. Les résultats de l'analyse peuvent être formatés de diverses façons, selon la configuration choisie par l'utilisateur, ce qui comprend entre autres des diagrammes des liens et des réseaux, des tableaux de bord, des cartes, des tableaux de bord personnalisables. Les données d'analytique peuvent être consultées par le GNCC et le partenaire. Différentes sections du GNCC (Section de la coordination opérationnelle, Section du renseignement, Section des conseils et de l'orientation en matière numérique) poursuivent leurs travaux ou s'acquittent de nouvelles tâches/entreprennent de nouveaux travaux à la lumière de cette analyse, par l'entremise du système de gestion des cas (attribution des tâches et flux des travaux).
La solution prototype devrait permettre au GNCC :
• De se connecter en toute sécurité à la solution. • De voir qu'il y a eu une CORRESPONDANCE SANS INTERVENTION quant à certaines données. • D'examiner et de valider l'information trouvée grâce aux corrélations et aux résultats des recherches. • D'attribuer le dossier à d'autres membres du groupe (traitement parallèle des tâches) ou de demander l'enrichissement des données par d'autres groupes que le GNCC. • De faire des recherches simultanément dans des sources de données internes et externes. • D'accéder aux résultats et de les configurer sous une variété de formats à l'aide de la fonction d'analytique.

- D'accéder aux tâches et aux flux des travaux du système de gestion des cas.

La solution prototype devrait permettre au partenaire de la police :

- De recevoir une notification par courriel pour l'informer qu'une trousse de renseignements est disponible sur le P3 et d'accéder à la trousse de renseignements préparée par la Section du renseignement.
- De se connecter en toute sécurité au P3.
- De recevoir des résultats sécurisés sous la forme d'une trousse de renseignements du GNCC.
- De faire une recherche dans les données découlant de l'analyse.
- D'accéder aux résultats et de les configurer sous une variété de formats à l'aide de la fonction d'analytique.
- De recevoir une CORRESPONDANCE SANS INTERVENTION.

Scénario 4 – Grille de notation

N° de l'indicateur		Indicateurs	Non établi (0)	Partiellement établi (3)	Établi en grande partie (6)	Pleinement établi (10)
Capacités	1	Permettre à l'utilisateur du GNCC de se connecter à la solution.	☐	☐	☐	☐
	2	Permettre à l'utilisateur du GNCC de voir une notification de CORRESPONDANCE SANS INTERVENTION.	☐	☐	☐	☐
	3	Permettre à l'utilisateur du GNCC de voir les résultats de la recherche qui ont été mis en correspondance.	☐	☐	☐	☐
	4	Permettre à l'utilisateur du GNCC d'envoyer une nouvelle demande à un autre utilisateur du GNCC.	☐	☐	☐	☐
	5	Permettre à un deuxième utilisateur du GNCC de faire une recherche « approximative » simultanément dans des sources internes et externes.	☐	☐	☐	☐
	6	La recherche « approximative » permet de relever une correspondance à l'égard d'une adresse IP, d'une adresse courriel, d'un sobriquet et d'une adresse bitcoin.	☐	☐	☐	☐

	7	Permettre à l'utilisateur de voir les données, y compris : • les diagrammes des liens et des autres réseaux; • les tableaux de bord; • les cartes; • les tableaux de bord personnalisables; • autres.	☐	☐	☐	☐
	8	Permettre à l'utilisateur du GNCC de préparer une réponse sous la forme d'une trousse de renseignements, y compris toute donnée supplémentaire, corrélation, analyse et conclusion (visualisations de données comprises).	☐	☐	☐	☐
	9	Permettre à l'utilisateur du GNCC d'envoyer une notification par courriel sécurisé à tous les organismes concernés pour les informer qu'une nouvelle trousse de renseignements est prête dans le Portail des partenaires et des policiers.	☐	☐	☐	☐
	10	Permettre à l'utilisateur du P3 d'accéder à la trousse de renseignements dans le P3.	☐	☐	☐	☐
	11	Permettre à l'utilisateur du P3 de faire une recherche en utilisant les critères énoncés dans la trousse de renseignements.	☐	☐	☐	☐
	12	Permettre à l'utilisateur du P3 d'accéder aux outils d'analytique sous plusieurs formats.	☐	☐	☐	☐
Note pour le scénario 4 :			**/120**			

Tableau A-7 : ECC – Scénario 5 – Intégration du signalement public

SCÉNARIO 5 – Intégration d'un signalement public **Thèmes du scénario :** Gestion de l'identité, intégration de l'interface de signalement public, Portail des partenaires et des policiers, matrice de gravité des plaintes du public, gestion des cas
Le site de signalement public générera des fichiers concernant les plaintes transmises par le public ou les entreprises. Les fichiers de plainte sont intégrés automatiquement à la SNC au moyen d'un flux de données provenant du site Web de signalement public. Récit de l'utilisateur Le GNCC a reçu cinq (5) signalements publics du site de signalement destiné au public. Le service de police compétent est le même dans les cinq cas, et celui-ci a indiqué que, pour les signalements publics, il souhaite recevoir les rapports qui ont un degré de priorité élevé. Le service a établi que les rapports concernant une perte de plus de 10 000 $ avaient un degré de priorité élevé. 1) Rapport A : contient des données qui figurent sur une « liste de surveillance des indicateurs de compromission » de la Section du renseignement du GNCC. 2) Rapport B : fournit des données sur un crime qui ne relève pas du mandat du GNCC. 3) Rapport C : signale un vol de 200 $ commis au moyen d'un rançongiciel. 4) Rapport D : signale un vol de 100 000 $ commis au moyen d'un rançongiciel. 5) Rapport E : signale une escroquerie par voie de mise à jour ou de réparation logicielle pour laquelle la victime a payé 250 $. Les rapports A, C et D seront intégrés à la SNC. Le rapport B sera traité comme une exception. La Section du renseignement, la Section de la réception et du triage et le service de police compétent accéderont tous à ces demandes et les géreront dans le système de gestion des cas de la SNC. Dans le cas du rapport D, on établit une correspondance avec une enquête menée par un partenaire international qui souhaite travailler avec différents partenaires (y compris la police canadienne) pour mener une enquête sur ce type particulier de rançongiciel. La solution soulignera cette correspondance à un analyste du GNCC et lui permettra d'ajouter cette information utile de façon à créer un rapport enrichi qui sera envoyé au service de police compétent partenaire. Le rapport E entre en corrélation avec plusieurs rapports existants. La solution tiendra compte de cette importante corrélation (p. ex. ampleur des préjudices, valeur totale de la perte financière) au moment d'établir la gravité et de souligner les corrélations à un analyste du GNCC.
La solution prototype devrait automatiquement :
• Recevoir les demandes par l'entremise du site de signalement destiné au public. • Intégrer les signalements publics. • Trier, analyser et évaluer les demandes et établir les correspondances.

- Identifier le service de police compétent en fonction de l'endroit.

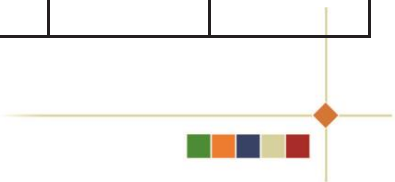
La solution prototype devrait permettre au GNCC :

- De se connecter en toute sécurité à la solution.
- D'évaluer les signalements publics.
- D'utiliser les règles relatives à la « liste de surveillance » pour envoyer une notification à la Section du renseignement en fonction des attributs de la demande.
- D'utiliser les règles relatives à l'exception pour aviser le groupe du fait que des données ne relevant pas de son mandat ont été traitées.
- De gérer l'exception – envoyer les signalements contenant des données ne relevant pas de son mandat à l'organisme approprié.
- D'utiliser l'échelle de gravité des plaintes du public pour établir l'ordre de priorité des signalements publics à transmettre au service de police compétent.
- D'aviser l'analyste des signalements publics du GNCC de la nécessité d'étayer le rapport à priorité élevée avant de le transmettre au service de police compétent.
- De créer et d'envoyer des notifications au service de police compétent.
- Autres

La solution prototype devrait permettre au partenaire de la police :

- De recevoir une notification par courriel l'informant que des signalements publics sont disponibles dans le P3.
- De se connecter en toute sécurité au P3.
- De configurer ses règles pour le filtre de gravité des plaintes du public.
- D'accéder à un tableau de bord permettant de visualiser les fichiers de plaintes du public, lequel est fondé sur les seuils configurables de visualisation des partenaires du P3.
- De choisir un signalement public pour voir les détails et peut-être les mesures prises.
- De permettre à l'utilisateur du P3 de télécharger le fichier de plainte du public.
- De permettre à l'utilisateur du P3 d'indiquer au GNCC qu'il ne peut pas procéder à un renvoi.
- De permettre à l'utilisateur du P3 d'indiquer au GNCC qu'il prend des mesures quant à un fichier de plainte du public.

Scénario 5 – Grille de notation						
N° de l'indicateur		**Indicateurs**	**Non établi (0)**	**Partiellement établi (3)**	**Établi en grande partie (6)**	**Pleinement établi (10)**
Capacités	**1**	Intégrer automatiquement les signalements publics.	☐	☐	☐	☐
	2	Établir automatiquement le degré de gravité, trier et analyser automatiquement les signalements publics, y compris les indicateurs de compromission, et établir automatiquement les correspondances.	☐	☐	☐	☐
	3	Établir automatiquement les correspondances entre une demande et une liste de surveillance du renseignement, et aviser le groupe responsable du renseignement.	☐	☐	☐	☐
	4	Attribuer automatiquement le billet au groupe de réception et de triage du GNCC aux fins de traitement.	☐	☐	☐	☐
	5	Établir automatiquement une exception à la lumière du mandat du GNCC (pour les signalements publics applicables) et permettre à l'utilisateur du GNCC d'envoyer un message à une autre section.	☐	☐	☐	☐
	6	Identifier automatiquement le service de police compétent en fonction de l'endroit, en utilisant le code postal fourni dans le signalement public.	☐	☐	☐	☐
	7	Pour le service de police compétent, afficher automatiquement le signalement public dans le P3 en fonction des filtres du service de police compétent relativement aux plaintes.	☐	☐	☐	☐
	8	Permettre à l'utilisateur du GNCC de se connecter en toute sécurité.	☐	☐	☐	☐
	9	Permettre à l'utilisateur du GNCC de voir les résultats des correspondances découlant des plaintes du public.	☐	☐	☐	☐
	10	Permettre à l'utilisateur du GNCC d'enrichir un fichier de plainte.	☐	☐	☐	☐
	11	Permettre à l'utilisateur du GNCC de joindre les résultats de l'enrichissement à la plainte.	☐	☐	☐	☐



	12	Permettre à l'utilisateur du P3 de se connecter en toute sécurité.	☐	☐	☐	☐
	13	Permettre à l'utilisateur du P3 de voir son tableau de bord et de faire défiler vers le bas pour consulter les plaintes du public relevant de sa compétence.	☐	☐	☐	☐
	14	Permettre à l'utilisateur du P3 de télécharger la plainte du public.	☐	☐	☐	☐
	15	Permettre à l'utilisateur du P3 d'informer la SNC des mesures prises ou de l'abandon de la plainte du public.	☐	☐	☐	☐
Note pour le scénario 5 :			**/150**			

Tableau A-8 : ECC – Évaluation selon l'échelle de convivialité du système (ECS)

ÉVALUATION DES CAPACITÉS ET DE LA CONVIVIALITÉ – PARTIE DEUX : ÉVALUATION SELON L'ÉCHELLE DE CONVIVIALITÉ DU SYSTÈME (ECS)					
Directives : Pour chacun des énoncés suivants, choisissez la case qui décrit le mieux votre réaction au prototype de solution nationale en matière de cybercriminalité.					
N° du scénario : _____ **Date :** _____/_____/_____					
N°	**Indicateur**	**Fortement en désaccord (1)**	**En désaccord (2)**	**En accord (4)**	**Fortement en accord (5)**
1	J'ai pu me connecter facilement au système.	☐	☐	☐	☐
2	Je peux facilement naviguer parmi les demandes.	☐	☐	☐	☐
3	Je peux facilement accéder à mes notifications et les consulter.	☐	☐	☐	☐
4	J'ai trouvé le clavardage en direct facile à utiliser et facile à naviguer.	☐	☐	☐	☐

5	Je peux facilement créer un projet.	☐	☐	☐	☐
6	Je peux facilement donner des tâches à d'autres personnes dans la solution.	☐	☐	☐	☐
7	Je peux facilement consulter les correspondances sans accusé de réception.	☐	☐	☐	☐
8	Je peux facilement visualiser ma file d'attente et mon tableau de bord et faire une recherche approfondie.	☐	☐	☐	☐
9	Je peux facilement utiliser la fonction de recherche et consulter les résultats.	☐	☐	☐	☐
10	Je peux facilement accéder à une trousse de renseignements et la consulter.	☐	☐	☐	☐
11	J'aimerais utiliser cette solution prototype fréquemment.	☐	☐	☐	☐
12	J'ai trouvé que la solution prototype était facile d'utilisation.	☐	☐	☐	☐
13	Je peux utiliser cette solution prototype sans assistance.	☐	☐	☐	☐
14	J'ai trouvé que les différentes fonctions de la solution prototype étaient bien intégrées.	☐	☐	☐	☐
15	J'estime qu'il y avait une cohérence dans cette solution prototype.	☐	☐	☐	☐
16	Je suis d'avis que la plupart des gens pourraient apprendre très rapidement à utiliser la solution prototype.	☐	☐	☐	☐
17	Je me suis senti très en confiance en utilisant la solution prototype.	☐	☐	☐	☐
NOTE GLOBALE DE L'ÉVALUATION SELON L'ÉCHELLE DE CONVIVIALITÉ DU SYSTÈME :				**/85**	

Tableau A-9 : ECC – Évaluation selon l'échelle de convivialité des fonctions d'accessibilité

ÉVALUATION DES CAPACITÉS ET DE LA CONVIVIALITÉ – PARTIE TROIS : ÉVALUATION SELON L'ÉCHELLE DE CONVIVIALITÉ DES FONCTIONS D'ACCESSIBILITÉ					
Directives : Pour chacun des énoncés suivants, choisissez la case qui décrit le mieux votre réaction au prototype de solution nationale en matière de cybercriminalité. Nous cherchons à évaluer l'accessibilité de la solution prototype pour les personnes qui utilisent des technologies d'assistance.					
Scénario : _____ **Date :** _____/_____/_____					
N°	**Indicateur**	**Fortement en désaccord (1)**	**En désaccord (2)**	**En accord (4)**	**Fortement en accord (5)**
1	Les images, les boutons et les graphiques disposaient d'un texte optionnel et étaient accessibles.	☐	☐	☐	☐
2	Il était facile de naviguer dans la solution prototype au moyen d'un clavier.	☐	☐	☐	☐
3	Le contenu était facile à lire, parce que le contraste était suffisant.	☐	☐	☐	☐
4	Le contenu était facile à lire, parce que la taille de la police était suffisante.	☐	☐	☐	☐
5	Le langage utilisé était simple, clair et facile à comprendre.	☐	☐	☐	☐
6	Les pages comportaient un titre approprié.	☐	☐	☐	☐
7	Les pages n'étaient pas surchargées, parce que la quantité de contenu sur chaque page était raisonnable.	☐	☐	☐	☐
8	Il était facile d'utiliser la solution prototype avec mon outil d'accommodement (le cas échéant).	☐	☐	☐	☐

9	La solution prototype a été conçue pour moi et mes besoins.	☐	☐	☐	☐
10	La solution prototype a été conçue pour répondre à la plupart des besoins et des exigences des employés sur les plans de l'accessibilité et de l'accommodement.	☐	☐	☐	☐
NOTE DE L' ÉVALUATION SELON L'ÉCHELLE DE CONVIVIALITÉ DES FONCTIONS D'ACCESSIBILITÉ				**/50**	

Tableau A-10 : ECC – Évaluation de l'innovation

ÉVALUATION DES CAPACITÉS ET DE LA CONVIVIALITÉ – PARTIE QUATRE : ÉVALUATION DE L'INNOVATION			
Le GNCC est à la recherche de technologies novatrices futures ou actuellement accessibles qui pourraient l'aider à s'acquitter de son mandat général. Les technologies novatrices proposées ne devraient pas se limiter à répondre aux exigences mentionnées; elles devraient permettre de répondre à des exigences qui n'ont pas encore été établies (conformément au MCO), afin d'aider le GNCC à réaliser sa mission. Les technologies novatrices des soumissionnaires seront évaluées en fonction des critères suivants : a) Comment la technologie et la fonctionnalité vont au-delà des capacités décrites dans le MCO; b) Un ou plusieurs exemples opérationnels, avec des détails suffisants, de la façon dont la nouvelle technologie ou l'innovation pourrait aider le GNCC à réaliser son mandat général et à atteindre l'un ou l'ensemble des quatre objectifs clés : i) Coordination et élimination des conflits ii) Production de renseignements qui permettent la prise de mesures iii) Conseils et orientation en matière numérique iv) Signalement public			
Critère n°		**Critère de réussite pour l'innovation**	**Note**
Capacités	**1**	Le soumissionnaire devrait documenter comment sa solution fournit une ou plusieurs technologies et fonctionnalités au-delà des capacités et des exigences mentionnées et décrites dans le MCO, de façon à aider le GNCC à réaliser sa mission. La description des capacités améliorées doit devrait être fournie au moyen d'un texte de 2 000 mots au maximum. A. Le soumissionnaire devrait mentionner clairement comment sa ou ses technologies ou fonctionnalités proposées vont au-delà des exigences mentionnées pour l'un ou plusieurs des objectifs clés énoncés dans le mandat du GNCC. c) Coordination et élimination des conflits	**Maximum de 100 points** A. 0 point Aucun renseignement n'a été fourni, ou des renseignements insuffisants ont été fournis pour permettre l'évaluation; aucune description fournis de comment la technologie et la fonctionnalité aideraient à atteindre les objectifs du GNCC; ou la technologie et la fonctionnalité décrites étaient déjà mentionnées dans le MCO. 25 points L'un des objectifs clés est abordé, et le soumissionnaire a fourni une description claire et concise ainsi qu'un exemple opérationnel d'une technologie et fonctionnalité actuellement disponibles et de

		d) Production de renseignements qui permettent la prise de mesures e) Conseils et orientation en matière numérique f) Signalement public **(maximum de 50 points)** B. Pour les futures fonctionnalités ou capacités, le soumissionnaire doit fournir une feuille de route publiée (qui a été fournie aux autres clients) qui décrit clairement les futures fonctionnalités et capacités. g) Coordination et élimination des conflits h) Production de renseignements qui permettent la prise de mesures i) Conseils et orientation en matière numérique j) Signalement public	la façon dont celles-ci peuvent aider le GNCC, et le besoin n'était pas mentionné dans le MCO. 50 points Deux des objectifs clés ou plus sont abordés, et le soumissionnaire a fourni une description claire et concise ainsi qu'un exemple opérationnel d'une technologie et fonctionnalité supplémentaires actuellement disponibles et de la façon dont celles-ci peuvent aider le GNCC, et le besoin n'était pas mentionné dans le MCO. B. 0 point Aucune feuille de route publiée n'a été fournie pour permettre l'évaluation ou aucun objectif n'a été abordé dans la feuille de route publiée, sans description claire et concise de la technologie ou de la fonctionnalité future abordée, ainsi que de la manière dont cette technologie ou fonctionnalité future aidera le GNCC. 25 points Dans la feuille de route publiée, l'un des objectifs clés est abordé, et le soumissionnaire a fourni une description claire et concise d'une technologie et fonctionnalité futures et de la façon dont celles-ci peuvent aider le GNCC. 50 points Dans la feuille de route publiée, deux des objectifs clés ou plus sont abordés, et le soumissionnaire a fourni une description claire et concise d'un autre type de technologie et fonctionnalité futures et de la façon dont celles-ci peuvent aider le GNCC
	2	Le soumissionnaire devrait démontrer la ou les technologies ou fonctionnalités novatrices actuellement accessibles intégrées dans son prototype et décrites au premier critère de réussite pour l'innovation. Le soumissionnaire devrait clairement démontrer comment la ou les technologies ou fonctionnalités existantes intégrées	**Maximum de 40 points** 0 point Le soumissionnaire n'a pas fourni de démonstration quant aux capacités améliorées décrites au premier critère d'évaluation.

		dans son prototype vont au-delà des exigences mentionnées à l'égard de l'un ou de plusieurs des quatre objectifs clés énoncés dans le mandat du GNCC. a) Coordination et élimination des conflits b) Production de renseignements qui permettent la prise de mesures c) Conseils et orientation en matière numérique d) Signalement public	10 points Il est clairement démontré que le prototype permet l'atteinte de l'un des objectifs clés.
NOTE GLOBALE OBTENUE À L'ÉVALUATION DE L'INNOVATION :			**/140**

Appendice B – Mobilisation des entrepreneurs de la SCN – Phase de prototype

B.1 Objet : Séances de mobilisation des entrepreneurs

a) L'approche d'élaboration de systèmes agiles exige une plus grande interaction avec les entrepreneurs pour produire de meilleurs résultats pour le groupe national de coordination contre la cybercriminalité (GNCC). Le gouvernement du Canada exige des entrepreneurs qu'ils comprennent parfaitement les exigences, qu'ils soient innovants et que les utilisateurs soient au premier plan. Le gouvernement du Canada exige que des séances de mobilisation des entrepreneurs soient organisées afin de leur fournir une rétroaction sur les prototypes au fur et à mesure de leur élaboration. Ces séances seraient menées de la même manière pour chaque entrepreneur afin de leur donner la même possibilité de faire des démonstrations et de demander une rétroaction ou une contribution à leur travail sur le prototype.

b) La portée des travaux relatifs à la solution prototype comprend la planification, la conception, le développement, la configuration, les essais et la livraison d'un plus petit produit viable (PPPV) de solution hébergée dans le nuage et fonctionnelle prenant en charge jusqu'à cent (100) utilisateurs, conformément aux exigences techniques et fonctionnelles requises décrites dans les présentes. La solution prototype ne doit pas nécessiter de modification importante entre l'évaluation ECC et le déploiement dans le cadre du test de prototype sur plateforme.

c) PPPV :

   i) **Description :** L'entrepreneur répond au minimum aux exigences des cinq (5) scénarios d'ECC (c'est-à-dire la solution prototype) dans la demande de propositions tel que décrit dans l'Appendice A – Évaluation des capacités et de la convivialité (ECC).

   ii) **Intention** : Permettre à l'entrepreneur de démontrer qu'il peut satisfaire à toutes les exigences de l'ECC, mais aussi, de démontrer toute fonctionnalité supplémentaire ou avancée dont son produit est capable dans les délais.

d) Test de prototype sur plateforme :

   i) **Description :** À la discrétion du Canada, réaliser un test de prototype sur plateforme de la solution de l'entrepreneur le mieux classé (déterminé pendant l'ECC) pour vérifier les exigences fonctionnelles et non fonctionnelles comme il est indiqué à la Section 2.5 – Test de prototype sur plateforme.

   ii) **Intention :** Veiller à ce que le prototype, lorsqu'il sera installé selon le modèle de services infonuagiques de l'entrepreneur, réponde aux exigences fonctionnelles et non fonctionnelles.

B.2 Concept des séances de mobilisation des entrepreneurs

a) Un minimum de trois (3) séances de mobilisation avec chaque entrepreneur sera organisé pendant la phase de prototype, pour un total de neuf (9) séances. À la discrétion du Canada, des séances de mobilisation supplémentaires peuvent être tenues, en nombres égaux, avec chaque entrepreneur. On s'attend à ce que chaque entrepreneur participe aux séances tout au long du processus d'élaboration du prototype.

b) Les trois (3) séances se tiendront au début, au milieu et à la fin de la phase de prototype. Les entrepreneurs et leurs prototypes ne seront pas évalués pendant les séances (c'est-à-dire que des notes selon l'ECC ne seront pas attribuées). L'objectif est de fournir une rétroaction et de répondre aux questions afin de permettre à l'entrepreneur de continuer à construire un meilleur prototype pour mieux répondre aux besoins du GNCC.

c) Il y aura des éléments et des règles communes qui s'appliqueront aux trois séances, mais les objectifs et la composition de chacune des séances seront légèrement différents, comme décrit ci-dessous.

B.2.1 Communs à toutes les séances

a) Chaque séance durera huit (8) heures et sera menée virtuellement avec des capacités de présentation et de multiples points de connectivité. Si des séances en personne sont possibles, elles pourraient être menées dans un bureau de la GRC situé dans la région de la capitale nationale.

b) Chaque séance permettra à l'entrepreneur de démontrer les capacités suivantes, en fonction des cas d'utilisation qui ont été fournis dans l'ECC, et d'obtenir des avis ou une rétroaction à leur sujet :

i) Gestion de cas;

ii) Portail des partenaires et des policiers;

iii) Intelligence artificielle, apprentissage automatique et traitement du langage naturel;

iv) Analyses.

c) La séance pourrait également permettre de discuter des capacités non fonctionnelles. Le Canada prévoit la présence d'experts en matière technique de la GRC lors des séances d'engagement afin de comprendre les prototypes des entrepreneurs et les exigences non fonctionnelles avant l'éventuel test de prototype sur plateforme.

B.2.2 Réponses à l'entrepreneur

a) Les informations exclusives d'un entrepreneur dans une question ne sont pas transmises à d'autres parties au cours d'un processus de Q et R. Les réponses (et les questions) du Canada à d'autres types de questions pourraient être communiquées directement aux autres entrepreneurs par l'autorité contractante afin de garantir la transparence et l'équité du processus. Toutes les réponses écrites aux questions des entrepreneurs passent par l'autorité contractante et sont documentées au dossier du contrat.

b) Étant donné que l'objectif des séances de mobilisation n'est pas d'évaluer officiellement les prototypes, le Canada ne fournira pas de note et ne confirmera pas officiellement si un élément démontré par un entrepreneur répond ou non à une exigence.

c) Le gouvernement du Canada fournira une rétroaction aux entrepreneurs de manière informelle en indiquant qu'ils sont « SUR LA BONNE VOIE », « PAS SUR LA BONNE VOIE » ou que le gouvernement du Canada est « INCAPABLE DE FOURNIR DES COMMENTAIRES POUR LE MOMENT ». Cette rétroaction ne constitue pas une évaluation officielle. L'évaluation formelle sera effectuée au cours du processus d'ECC.

i) SUR LA BONNE VOIE : correspond aux capacités fonctionnelles décrites dans l'ECC.

ii) PAS SUR LA BONNE VOIE : ne correspond pas aux capacités fonctionnelles décrites dans l'ECC.

iii) INCAPABLE DE FOURNIR DES COMMENTAIRES POUR LE MOMENT : pas assez de détails pour faire des commentaires.

d) Quelle que soit la rétroaction fournie, le gouvernement du Canada ne sera pas tenu responsable de la rétroaction pendant le processus formel d'ECC (par exemple, le gouvernement du Canada pourrait indiquer comme rétroaction pendant les séances d'engagement qu'une exigence est jugée « SUR LA BONNE VOIE », mais réaliser ensuite pendant l'ECC que l'entrepreneur n'a pas satisfait à l'exigence sur la base d'une évaluation plus complète et du fait que beaucoup de choses pourraient changer entre la démonstration et l'évaluation formelle).

e) En ce qui concerne la rétroaction recherchée sur la convivialité, l'apparence et la présentation, les réponses se limiteront à « CORRESPOND AUX ATTENTES », « NE CORRESPOND PAS AUX ATTENTES » ou « INCAPABLE DE FOURNIR DES COMMENTAIRES POUR LE MOMENT ».

i) CORRESPOND AUX ATTENTES : convivial.

ii) NE CORRESPOND PAS AUX ATTENTES : non convivial.

iii) INCAPABLE DE FOURNIR DES COMMENTAIRES POUR LE MOMENT : pas assez de détails pour faire des commentaires.

B.2.3 Processus de mobilisation des entrepreneurs

a) Les procédures suivantes décrivent les étapes et les garanties à suivre lors des séances de mobilisation des entrepreneurs qui auront lieu pendant la phase de prototype du développement de la SNC.

i) L'entrepreneur doit fournir un aperçu préalable de ce qu'il prévoit de démontrer lors de chaque séance. L'aperçu doit être fourni à la GRC au moins trois (3) jours ouvrables avant la démonstration afin que la GRC puisse s'assurer que les experts pertinents sont présents pendant la séance.

ii) Pendant la démonstration, la GRC pourrait avoir l'occasion de « signaler » à l'entrepreneur que des questions seront posées sur un certain sujet.

iii) Il pourrait y avoir une pause dans la séance afin de permettre une brève discussion entre les principaux représentants de la GRC.

iv) La séance de Q et R permettra une interaction entre la GRC et l'entrepreneur, où chaque partie pourra poser des questions et y répondre. Toutes les questions et réponses seront consignées par des préposés au registre des communications pour la tenue des dossiers.

v) L'entrepreneur peut consulter sa solution prototype ou choisir d'en faire une nouvelle démonstration lorsqu'il répond aux questions de la GRC.

vi) Toute question de l'entrepreneur à laquelle la GRC ne peut pas répondre directement pendant la séance de Q et R sera placée dans une liste de questions en suspens et fera l'objet d'une réponse par écrit dans les cinq (5) jours ouvrables suivant la démonstration. La GRC se réserve le droit de décider quelles questions elle souhaite placer dans la liste de questions en suspens pendant la séance.

vii) Toute question de la GRC à laquelle l'entrepreneur ne peut pas répondre directement sera placée dans une liste de questions en suspens, et fera l'objet d'une réponse par écrit dans les cinq (5) jours ouvrables suivant la démonstration. L'entrepreneur se réserve le droit de décider quelles questions il souhaite placer dans la liste de questions en suspens pendant la séance. La GRC ne répondra aux questions et ne communiquera des informations qu'en fonction de la classification de sécurité des informations qu'elle est autorisée à communiquer à ce stade du processus.

viii) L'entrepreneur recevra une transcription écrite des questions et réponses dans les cinq (5) jours ouvrables suivant la démonstration.

ix) Les questions et réponses de nature exclusive, telles qu'indiquées par l'entrepreneur dans sa réponse, ne seront pas transmises aux autres entrepreneurs du prototype. Les questions et réponses qui ne sont pas de nature exclusive seront transmises aux autres entrepreneurs du prototype.

B.3 Concept pour la séance 1

Tableau B-1 : Concept pour la séance 1

Échéancier	5 semaines après le début du processus de prototype		
Objectif	Une démonstration générale, tôt dans le processus, du travail effectué jusqu'à cette date. Démonstration moins axée sur la convivialité, et plus sur les technologies utilisées et les concepts généraux, la GRC fournissant une rétroaction.		
Journée de mobilisation de l'industrie	Matin et début d'après-midi	Démonstrations générales de l'entrepreneur, questions ou demande de rétroaction; il n'est pas nécessaire d'aborder des cas d'utilisation et certaines capacités spécifiques.	6 heures
	Après-midi	Questions de la GRC et rétroaction non sollicitée.	2 heures

B.4 Concept pour la séance 2

Tableau B-2 : Concept pour la séance 2

Échéancier	10 semaines après le début du processus de prototype		
Objectif	L'objectif de la deuxième séance est que l'entrepreneur fasse une démonstration de quatre (4) capacités au maximum et de leur fonctionnement en relation avec les cas d'utilisation. Cette séance devrait au minimum comprendre une démonstration du portail des partenaires et des policiers et de la gestion de cas. Il appartient à l'entrepreneur de déterminer s'il fera la démonstration des quatre (4) capacités (voir B.2.1 b)) et de tous les scénarios. Cette séance devrait comprendre des démonstrations et des explications plus détaillées et en direct des fonctions ou des exigences de chacune des quatre (4) capacités. La présentation visuelle de la deuxième séance devrait comporter plusieurs écrans afin que les examinateurs puissent voir les détails de près.		
Journée de mobilisation de l'industrie	Matin	Démonstrations de l'entrepreneur, questions ou demande de rétroaction. Doit couvrir au moins les capacités de la deuxième séance.	4,5 heures
	Après-midi	Permettre aux experts du GNCC de se concentrer sur les capacités de gestion de cas et aux experts des partenaires policiers de se concentrer sur le portail des partenaires et des policiers. Deux demandes	1,5 heure

Tableau B-2 : Concept pour la séance 2

		supplémentaires pour que l'entrepreneur démontre certains aspects de cette capacité seront autorisées pendant cette tranche horaire.	
	Après-midi	La GRC doit demander une démonstration sur certains éléments (comprend le temps nécessaire pour la démonstration elle-même).	1 heure
	Après-midi	Questions de la GRC et rétroaction non sollicitée.	1 heure

B.5 Concept pour la séance 3

Tableau B-3 : Concept pour la séance 3

Échéancier	15 semaines après le début du processus de prototype		
Objectif	L'objectif de la troisième séance est que l'entrepreneur fasse une démonstration complète des quatre (4) capacités et de leur fonctionnement en relation avec les cas d'utilisation. Cela devrait comprendre une démonstration des quatre (4) capacités ainsi qu'une partie interactive où les experts du GNCC et des partenaires policiers peuvent utiliser le prototype avec un représentant de l'entrepreneur qui les guide. Cet élément permettra aux experts en la matière d'utiliser la gestion de cas, le portail des partenaires et des policiers, l'intelligence artificielle, l'apprentissage automatique et le traitement du langage naturel, ainsi que les fonctions d'analyse. Les technologies innovantes (quatrième partie de l'ECC) peuvent également être présentées lors de cette séance. Il n'est pas nécessaire que les démonstrations couvrent tout le matériel démontré précédemment. Cette séance devrait se concentrer sur des démonstrations et des explications assez détaillées et en direct des fonctions ou des exigences de chacune des quatre (4) capacités. Cette séance doit permettre aux experts du GNCC et des partenaires policiers de travailler avec le prototype et de faire fonctionner le système avec l'aide d'un représentant de l'entrepreneur. Cette séance sera principalement réalisée de manière virtuelle.		
Journée de mobilisation de l'industrie	Matin	L'entrepreneur doit faire des démonstrations générales, poser des questions ou demander une rétroaction sur les quatre (4) capacités. Si une (ou plusieurs) technologie innovante doit faire l'objet d'une démonstration (partie 4	2 heures

Tableau B-3 : Concept pour la séance 3

		de l'ECC), celle-ci doit avoir lieu pendant cette tranche horaire.	
	Après-midi	Permettre aux experts du GNCC et des partenaires policiers de mettre à l'essai le portail des partenaires et des policiers. Des demandes supplémentaires pour que l'entrepreneur démontre certains aspects de cette capacité seront autorisées pendant cette tranche horaire.	1,5 heure
	Après-midi	Permettre aux experts du GNCC et des partenaires policiers de mettre à l'essai la fonction d'analyse. Des demandes supplémentaires pour que l'entrepreneur démontre certains aspects de cette capacité seront autorisées pendant cette tranche horaire.	1,5 heure
	Après-midi	La GRC peut demander une démonstration sur certains éléments (comprend le temps nécessaire pour la démonstration elle-même).	45 minutes

Appendice C – Modèle de capacité opérationnelle de la SNC

a) On a élaboré le Modèle de capacité opérationnelle de la SNC (le MCO de la SNC) pour décrire la portée complète des services et des capacités de la solution qui sont requis pour permettre la prestation des services opérationnels du GNCC.

b) Le MCO de la SNC comprend les éléments suivants :

   i) un diagramme général montrant les principales capacités opérationnelles, ainsi que les capacités fonctionnelles et techniques de soutien de la solution;

   ii) des diagrammes de décomposition fonctionnelle;

   iii) des descriptions des capacités sous la forme de tableaux.

C.1 Modèle de capacité de la Solution nationale en matière de cybercriminalité

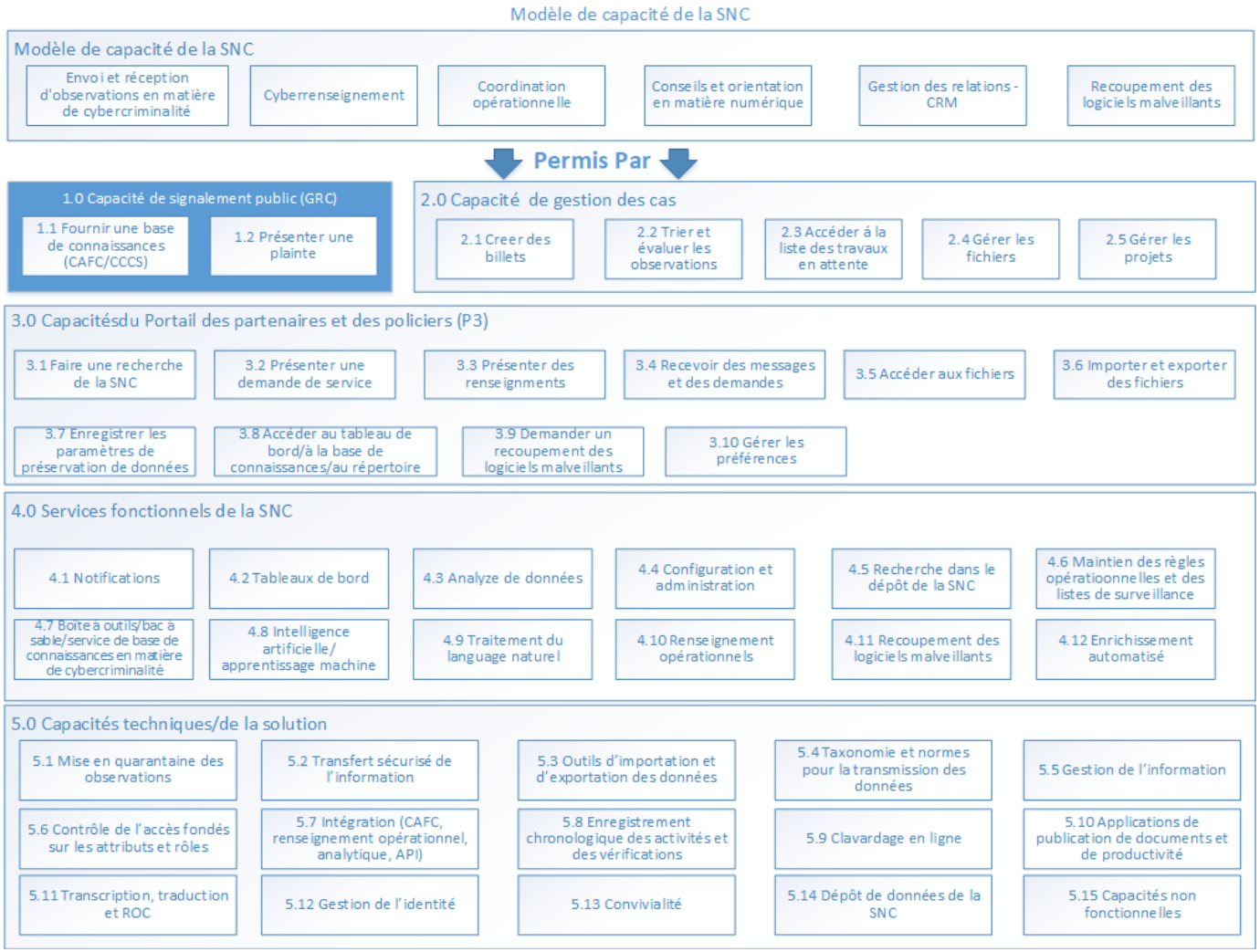


Figure C-1 : Modèle de capacité de la SNC

C.2 SNC – Capacités de signalement public

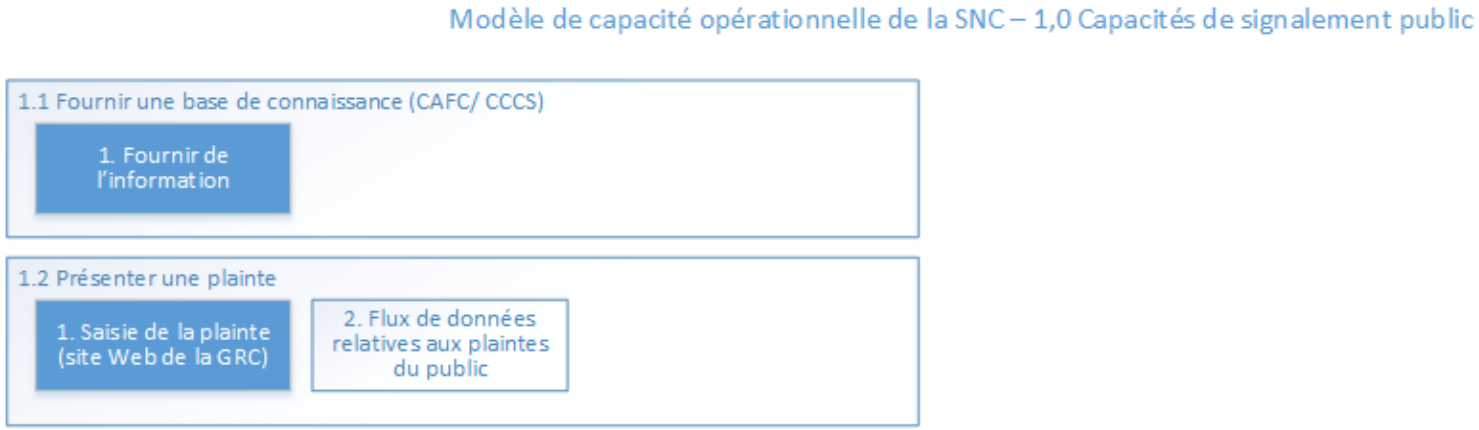


Figure C-2 : SNC – Capacités de signalement public

Tableau C-1 : SNC – Capacités de signalement public

1.2 Traitement des plaintes Le système intégrera automatiquement les signalements publics en matière de cybercriminalité et de fraude qui ont été reçus par l'entremise du site Web de signalement public.	
1.2.2 Flux de données relatif aux plaintes du public	
1.2.2.1	La solution doit charger les fichiers de plaintes du public qui ont été traitées par le SNSCF.

C.3 SNC – Capacités de gestion des cas

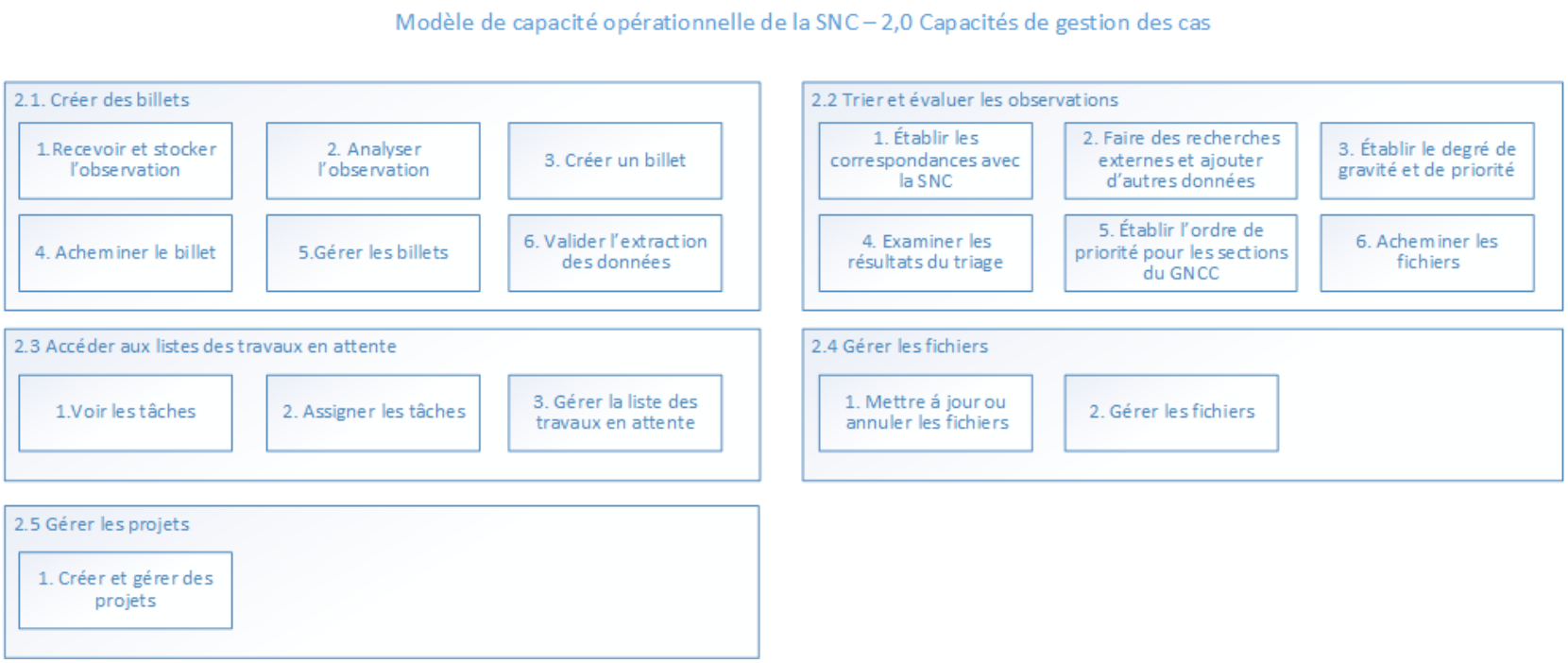


Figure C-3 : SNC – Capacités de gestion des cas

Tableau C-2 : SNC – Capacités de gestion des cas

2.1 Créer des billets Le système intégrera automatiquement les courriels pour créer des billets et permettra aux utilisateurs de créer des billets au moyen d'une interface de l'utilisateur. Dans le cadre de la création automatique d'un billet, le système analysera l'information et remplira les champs applicables pour créer le billet. Le cas échéant, les billets seront automatiquement transmis. Les billets peuvent être trans mis manuellement lorsque la transmission automatique ne s'applique pas. La solution créera des billets en fonction des documents transmis sur le P3 et des fichiers de plaintes du public reçues par l'entremise du Portail.	
2.1.1 Recevoir et stocker l'observation	
2.1.1.1	La solution doit stocker toutes les observations (y compris les fichiers de signalement public) et demandes de service, y compris toute pièce jointe applicable, au fur et à mesure de leur réception, dans un format de lecture seule.
2.1.1.2	La solution doit automatiquement créer et stocker une version hachée de chaque observation, demande de service ou pièce jointe reçue.
2.1.1.3	La solution doit stocker automatiquement toutes les métadonnées des observations ou des demandes de service.
2.1.1.4	La solution doit, soit par l'utilisation des outils dans l'espace infonuagique de la GRC ou des produits fournis par l'entrepreneur, garantir que toutes les interfaces qui permettent l'ingestion de données ont des capacités adéquates de détection et d'élimination des logiciels malveillants.
2.1.1.5	La solution doit traiter automatiquement les observations reçues par l'entremise du P3. Le P3 applique les validations et utilise des modèles pour consigner les données dès leur entrée dans le système. Par conséquent, la SNC peut utiliser ces champs associés aux règles opérationnelles et aux règles liées au flux des travaux.
2.1.1.6	La solution doit analyser les observations pour détecter tout document montrant une situation d'exploitation et isoler ce document du reste du dossier jusqu'à son examen. Par exemple, une pièce jointe contenant une image montrant l'exploitation d'un enfant peut être détectée et renvoyée aux fins d'un examen manuel par des utilisateurs autorisés sélectionnés.
2.1.1.7	La solution doit créer un signet comportant un numéro de référence et une explication pour le retrait, relativement à toute partie de l'observation qui a été retirée (p. ex. document montrant une situation d'exploitation, logiciel malveillant).
2.1.2 Analyser l'observation	
2.1.2.1	La solution doit analyser automatiquement les observations et les demandes de service, y compris les métadonnées et les indicateurs de compromission liés à la cybercriminalité.
2.1.2.2	La solution doit classer les observations ou les demandes de service selon leur type pour faciliter la transmission (p. ex., par type de crime).
2.1.2.3	La solution doit valider l'exhaustivité des observations et établir si toute l'information requise est fournie dans une observation ou une demande de service et si tous les champs, comme les dates, les codes postaux, les villes et la province, sont valides et bien formatés.

Tableau C-2 : SNC – Capacités de gestion des cas

2.1.2.4	La solution doit calculer la valeur monétaire en dollars canadiens en fonction du taux de change en vigueur au moment de la consignation des données. Cela comprend la cryptomonnaie et la monnaie fiduciaire.
2.1.2.5	La solution doit être en mesure d'analyser l'information figurant dans des images ainsi que dans des zones de texte.
2.1.2.6	La solution doit effectuer une validation par recoupement pour cerner les observations qui contiennent des renseignements incohérents dans des zones de texte relativement à des champs précis.
2.1.3 Créer un billet	
2.1.3.1	La solution doit être en mesure de créer un billet en fonction des données soumises par l'entremise du P3 et du site Web de signalement destiné au public.
2.1.3.2	La solution doit attribuer un numéro de référence unique du GNCC à chaque billet.
2.1.3.3	La solution doit permettre à l'utilisateur de créer un billet en utilisant des modèles pouvant être sélectionnés.
2.1.3.4	La solution doit automatiquement lier au billet toutes les pièces jointes, les données consignées et les métadonnées.
2.1.3.5	La solution doit permettre à l'utilisateur du GNCC d'examiner les billets créés automatiquement pour confirmer et approuver l'analyse et le contenu et pour modifier le billet si des corrections doivent être apportées.
2.1.3.6	La solution doit valider les billets créés par les utilisateurs pour garantir que toute l'information requise est présente et que les champs, comme les dates, les codes postaux, les villes et la province, sont valides et bien remplis.
2.1.3.7	La solution doit permettre la création de billets préremplis à l'aide d'un numéro de téléphone reçu par l'intermédiaire de l'interface de données téléphoniques du Centre d'appels.
2.1.3.8	La solution doit permettre à l'employé du GNCC qui prend l'appel de compléter le billet préremplien fonction de l'information reçue durant l'interaction téléphonique.
2.1.4 Acheminer le billet	
2.1.4.1	La solution doit acheminer automatiquement les billets à la section responsable de la prochaine étape (Section du triage et de l'évaluation ou une autre section compétente du GNCC) à l'aide des règles opérationnelles configurables (p. ex. une demande de conseils sera envoyée à la Section des conseils et de l'orientation techniques, une demande de préservation des données provenant d'un partenaire international sera soumise à l'équipe responsable du réseau, laquelle est disponible 24 heures sur 24, 7 jours sur 7, et une exception sera soumise à l'utilisateur responsable du traitement des exceptions).
2.1.4.2	La solution doit être en mesure d'acheminer automatiquement et manuellement les billets au sein du GNCC en fonction des règles configurables liées au flux des travaux.
2.1.4.3	La solution doit être en mesure d'acheminer un billet à un superviseur aux fins du traitement et de l'examen d'une exception (p. ex. menaces, hors de la portée du mandat, autres règles relatives à l'exception)
2.1.5 Gérer les billets	

Tableau C-2 : SNC – Capacités de gestion des cas

2.1.5.1	La solution doit permettre aux utilisateurs de gérer les billets au moins grâce aux fonctions suivantes : a. Rechercher b. Modifier c. Annuler d. Ajouter des renseignements e. Ajouter des pièces jointes f. Fusionner et défusionner g. Fractionner h. Réacheminer i. Imprimer
2.1.6 Valider l'extraction de données	
2.1.6.1	La solution doit fournir à l'utilisateur la capacité d'examiner et de modifier un billet (p. ex. corriger les champs remplis automatiquement durant l'analyse et apporter toute autre modification requise, y compris modifier la catégorie du billet).
2.1.6.2	La solution doit permettre à l'utilisateur d'analyser et de modifier manuellement les indicateurs de compromission et les données observables en matière de cybercriminalité à partir des observations et des pièces jointes, y compris le texte tiré des images jointes.
2.1.6.3	La solution doit permettre à l'utilisateur de remplir le répertoire des partenaires au moyen des coordonnées extraites automatiquement.
2.2 Trier et évaluer les observations On établira les correspondances entre les billets et les données stockées dans le dépôt de la SNC, et des recherches seront lancées pour enrichir l'observation. Les billets qui passent par l'étape de l'enrichissement sont par la suite appelés des fichiers. Après chaque stade de l'enrichissement, le fichier créé sera trié (noté), et on l'évaluera pour établir les prochaines étapes. En outre, les règles opérationnelles de la Section du renseignement et de la Section de la coordination opérationnelle sont appliquées aux fichiers, ce qui permet de savoir si ces sections doivent travailler sur un fichier.	
2.2.1 Établir les correspondances avec la SNC	
2.2.1.1	La solution doit établir automatiquement les correspondances entre les données du billet et les données existantes dans le dépôt des données en matière de cybercriminalité de la SNC et stocker automatiquement les résultats avec le billet.
2.2.1.2	La solution doit automatiquement déclencher l'envoi de notifications aux parties concernées si des correspondances sont relevées.
2.2.1.3	S'il est établi qu'un nouveau billet est lié à un billet existant (p. ex. il découle d'une demande de renseignements supplémentaires ou de précisions), la solution doit fusionner le billet et le billet initial.
2.2.1.4	La solution doit fournir des méthodes avancées et souples de mise en correspondance qui comprennent, sans s'y limiter, l'un ou l'autre des paramètres suivants ou une combinaison de ceux-ci :

Tableau C-2 : SNC – Capacités de gestion des cas

	a. mot ou expression exacts; b. synonymes; c. recherche approximative (p. ex. Soundex); d. mots occultés (p. ex. pirate = p1r4t3, captain = c4pt41n, disco = d1$c0, mysite.com = mysite dot com); e. sujets; f. outils, techniques et processus; g. expression rationnelle (configurable)
2.2.1.5	La solution doit établir des correspondances entre les données des billets du Centre d'appels et les données de signalements publics (p. ex. numéro de téléphone). En cas de correspondance, le nouveau billet sera prérempli à l'aide des données existantes, et les billets antérieurs pertinents seront à la disposition de la personne qui prend l'appel.
2.2.1.6	La solution doit être capable d'établir automatiquement les correspondances interlinguistiques avec des données reçues ou stockées dans plusieurs langues.
2.2.2 Faire des recherches externes et ajouter d'autres données	
2.2.2.1	La solution doit permettre à l'utilisateur d'enregistrer ses activités de recherche ainsi que ses activités d'enrichissement liées à des sources externes, comme Intelex, le SIRPP, le Centre canadien pour la cybersécurité (CCCS), le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), en plus de ses recherches dans des sources ouvertes ou d'autres sources de données externes.
2.2.2.2	La solution doit permettre à l'utilisateur de lier tous les résultats des recherches externes ou des activités d'enrichissement au fichier visé (p. ex. prendre des notes ou joindre les résultats sous forme de fichiers PDF, de fichiers texte ou d'images).
2.2.2.3	La solution doit permettre à un utilisateur de créer une demande d'information et de la transmettre à un ou plusieurs partenaires du P3.
2.2.3 Établir le degré de gravité et de priorité	
2.2.3.1	La solution doit utiliser les règles opérationnelles pour établir le degré de gravité du fichier et son ordre de priorité.
2.2.3.2	La solution doit utiliser le contenu du fichier et les résultats de chacune des étapes d'enrichissement, ainsi que les règles opérationnelles, afin d'établir le degré de gravité du fichier. La note et le degré de gravité du fichier peuvent changer après la réception et le traitement de chaque résultat.
2.2.3.3	La solution doit permettre à l'utilisateur d'effectuer d'autres activités d'enrichissement au besoin.
2.2.4 Examiner les résultats du triage	
2.2.4.1	La solution doit permettre à l'utilisateur d'examiner les résultats des mises en correspondance et des recherches dans les systèmes externes.
2.2.5 Établir l'ordre des priorités pour les sections du GNCC	

Tableau C-2 : SNC – Capacités de gestion des cas

2.2.5.1	La solution doit identifier les observations qui présentent un intérêt pour les sections du GNCC (p. ex. Section du renseignement, Section de la coordination opérationnelle), à l'aide de ce qui suit : a. les résultats de la mise en correspondance avec les données sur la cybercriminalité figurant dans le dépôt de la SNC - y compris les correspondances avec des travaux en cours au sein d'une section ou les correspondances avec des données précises figurant sur une liste de surveillance b. d'autres règles opérationnelles
2.2.6 Acheminer le fichier	
2.2.6.1	La solution doit être en mesure d'aviser automatiquement la Section du renseignement ou la Section de la coordination opérationnelle lorsque des fichiers ont atteint un seuil configurable, conformément aux règles d'établissement des priorités de chacune de ces sections.
2.2.6.2	La solution doit permettre aux utilisateurs de renvoyer manuellement un fichier à une autre section du GNCC aux fins de l'achèvement du traitement.
2.2.6.3	La solution doit permettre à la Section du renseignement ou à la Section de la coordination opérationnelle d'attribuer de façon anticipée un fichier durant le processus de triage et d'évaluation.
2.2.6.4	La solution doit acheminer les observations qui échappent peut-être à la portée du mandat du GNCC vers un processus de traitement des exceptions.
2.2.6.5	La solution doit être en mesure de rendre automatiquement les fichiers accessibles au service de police compétent.
2.3 Accéder aux listes des travaux en attente La solution fournira une fonctionnalité configurable permettant d'établir une liste des travaux afin que les utilisateurs du GNCC puissent gérer la charge de travail. Les listes des travaux en attente faciliteront l'attribution des tâches et l'accès aux tâches pour les différentes sections du GNCC. Les listes des travaux en attente peuvent contenir des attributions (tâches) liées aux billets, aux fichiers ou aux projets.	
2.3.1 Voir les tâches	
2.3.1.1	La solution doit permettre à l'utilisateur d'accéder aux listes des travaux en attente qui contiennent les tâches qui leur sont assignées ou d'accéder à un bassin de travaux à partir duquel ils peuvent choisir leurs tâches.
2.3.1.2	La solution doit permettre aux utilisateurs qui consultent les tâches de faire défiler vers le bas pour avoir accès à des détails ainsi qu'aux autres fonctionnalités dont ils ont besoin pour s'acquitter des tâches applicables.
2.3.1.3	La solution doit permettre à l'utilisateur de filtrer et de classer les tâches figurant dans une liste des travaux en attente ainsi que d'effectuer une recherche dans cette liste.
2.3.1.4	La solution doit permettre aux utilisateurs de voir leurs tâches en affichant différents niveaux de détail (p. ex. affichage du fichier ou d'un résumé du fichier au moment de visualiser les tâches).
2.3.2 Assigner les tâches	

Tableau C-2 : SNC – Capacités de gestion des cas

2.3.2.1	La solution doit permettre aux utilisateurs autorisés d'assigner des tâches en choisissant une tâche dans le bassin des travaux en attente d'une section et en la transférant vers la liste des travaux en attente d'une personne, qui peut ensuite accéder à la tâche au moyen de sa propre liste personnelle des travaux en attente.
2.3.2.2	La solution doit permettre aux utilisateurs de retirer une tâche d'une liste de tâches.
2.3.2.3	La solution doit permettre de filtrer les tâches en fonction d'attributs comme le type de crime ou le type de demande de service (p. ex. filtrage thématique), afin de permettre aux travailleurs de se concentrer sur des types de tâches précis.
2.3.2.4	La solution doit être en mesure de configurer les listes des travaux en attente pour permettre l'autoattribution de tâches ou l'attribution de tâches par le superviseur.
2.3.3 Gérer la liste des travaux en attente	
2.3.3.1	La solution doit permettre à l'utilisateur de réassigner une tâche à un autre employé ou de renvoyer une tâche dans le bassin de tâches de la section.
2.3.3.2	La solution doit permettre à l'utilisateur de rédiger une note quant à une tâche ou de fixer une date future pour la réalisation de la tâche. Une notification de la liste des travaux en attente fournira un rappel aux utilisateurs quant aux tâches associées à une date à venir.
2.3.3.3	La solution doit afficher les mêmes colonnes, selon le même ordre de tri et le même niveau de détail, que lorsque la liste des travaux en attente a été visionnée pour la dernière fois par l'utilisateur.
2.3.3.4	La solution doit permettre l'utilisation de modèles flexibles relativement aux flux des travaux (flux des travaux séquentiels, parallèles ou mixtes). Par exemple, des fichiers de la Section de la réception peuvent être attribués à la Section du renseignement ou la Section de la coordination opérationnelle, ou, advenant une exception en raison de contenu VIP, les fichiers peuvent être renvoyés au superviseur aux fins de traitement.
2.3.3.5	La solution doit permettre à l'utilisateur de changer le statut d'une tâche (p. ex. en cours d'examen, terminée, rejetée).
2.4 Gérer les fichiers Les billets deviennent des fichiers dès qu'une activité d'enrichissement manuel est exécutée par un utilisateur du GNCC, ou si le degré de gravité du billet dépasse un seuil configurable qui exige un examen manuel. Un fichier peut découler d'un ou de plusieurs billets. Les fichiers peuvent être mis à jour, de nouveaux liens vers d'autres fichiers ou billets peuvent être créés, et les fichiers peuvent être renvoyés à des sections internes du GNCC ou à des partenaires externes pour la prise de mesures supplémentaires.	
2.4.1 Mettre à jour ou annuler un fichier	
2.4.1.1	La solution doit permettre aux utilisateurs de gérer, de mettre à jour ou d'annuler un billet ou un fichier (p. ex. corriger des renseignements, ajouter de nouveaux renseignements, annuler, bloquer).
2.4.1.2	La solution doit aviser les parties concernées (p. ex. les sections du GNCC ou les organismes désignés) si de nouveaux renseignements sont ajoutés à un fichier et que le fichier est traité ou surveillé par une section du GNCC.

Tableau C-2 : SNC – Capacités de gestion des cas

2.4.1.3	La solution doit être en mesure d'attribuer un identificateur unique à un fichier.
2.4.1.4	La solution doit, lorsque plusieurs fichiers sont liés, permettre d'indiquer quel fichier est le fichier principal.
2.4.1.5	La solution doit permettre aux utilisateurs de gérer les fichiers, y compris de voir et d'imprimer le contenu, d'apporter des corrections, d'ajouter de nouveaux renseignements ou de nouvelles pièces jointes, d'ajouter des notes au fichier, d'établir un lien avec d'autres fichiers, d'ajouter des tâches et de renvoyer le fichier à d'autres sections du GNCC ou à des organismes externes.
2.4.1.6	La solution doit être en mesure de maintenir le statut des fichiers.
2.4.2 Gérer les fichiers	
2.4.2.1	La solution doit permettre de gérer tous les aspects des fichiers tout au long d'un cycle de vie complet (p. ex. créer, évaluer, modifier, en cours, renvoyé, terminé, archivé).
2.4.2.2	La solution doit permettre de renvoyer des fichiers à d'autres sections du GNCC ou à des partenaires externes et de recevoir des fichiers d'autres sections du GNCC (au moyen du P3).
2.4.2.3	La solution doit permettre à l'utilisateur d'accéder à des versions antérieures des champs et des pièces jointes des fichiers et de visionner ces champs (p. ex. si les données ont été manipulées aux fins de l'analyse ou si un champ a été modifié).
2.4.2.4	La solution doit permettre de gérer tous les aspects des fichiers de préservation des données tout au long d'un cycle de vie complet, y compris en préservant le lien entre la demande et l'ordonnance jusqu'au recours au Traité d'entraide juridique, au besoin.
2.4.2.5	La solution doit permettre à l'utilisateur de créer une trousse de l'« observation » renfermant tout le contenu et toutes les activités liés à un billet, à un fichier ou à un projet, y compris l'ensemble des données, des métadonnées, des journaux d'activités, des journaux de vérification de système et des pièces jointes.
2.4.2.6	La solution doit permettre à l'utilisateur d'imprimer tout élément du fichier en l'envoyant à l'imprimante ou en imprimant vers un fichier (p. ex. PDF).
2.4.2.7	La solution doit appliquer les désignations configurables relatives à la sécurité de l'information et respecter les protocoles de partage en fonction du niveau attribué pour tous les extrants.
2.4.2.8	La solution doit permettre à l'analyste d'ajouter des filigranes configurables (p. ex. « Confidentiel », « La règle relative aux tiers s'applique », « Protégé B ») à tous les extrants.
2.4.2.9	La solution doit permettre à l'utilisateur de trouver et d'examiner les fichiers sans égard au statut (selon le contrôle d'accès basé sur les rôles et le contrôle d'accès basé sur les attributs), sans que le fichier lui ait été attribué.
2.4.2.10	La solution doit permettre à l'utilisateur de créer une valeur de hachage pour tout rapport ou toute pièce jointe et de communiquer la valeur de hachage avec le rapport ou la pièce jointe visés.
2.4.2.11	La solution doit permettre de gérer les listes de distribution liées à un fichier ou à un projet pour soutenir la diffusion des rapports, des trousses de divulgation ou d'autres extrants liés au fichier ou au projet. La publication individuelle ou en lots de trousses, de

Tableau C-2 : SNC – Capacités de gestion des cas

	rapports et de notifications doit pouvoir se faire par courriel ou au moyen du P3. Les listes de distribution ne doivent pas être limitées (p. ex. elles peuvent comprendre des partenaires du P3, des victimes, d'autres ministères, des organisations du secteur privé).
2.5 Gérer les projets Créer et maintenir un projet pour établir un lien entre les fichiers, les données, les organismes concernés et les résultats connexes. Un projet aidera les utilisateurs concernés à gérer les activités et les tâches reliées. L'accès à un projet peut être limité à des utilisateurs ou à des groupes précis. Les exigences relatives à l'impression et au contrôle sont les mêmes que pour les fichiers, mais à l'échelon des projets.	
2.5.1 Créer et gérer des projets	
2.5.1.1	La solution doit permettre de créer et de gérer un projet en enregistrant l'information pertinente, comme les fichiers connexes, le type de projet, le sommaire, la date, le degré de priorité, les utilisateurs concernés, les groupes concernés, les organismes concernés, le nom du projet, le statut et les activités, entre autres.
2.5.1.2	La solution doit attribuer un numéro de projet unique au projet.
2.5.1.3	La solution doit permettre d'imprimer le contenu d'un projet et offrir toutes les fonctionnalités liées à l'impression d'un fichier; en plus de permettre de créer une trousse de divulgation à l'échelon du projet.
2.5.1.4	La solution doit permettre de gérer tous les aspects du projet tout au long d'un cycle de vie complet (p. ex. créer, évaluer, modifier, en cours, renvoyé, terminé, archivé).
2.5.1.5	La solution doit permettre d'affecter des utilisateurs à un projet.
2.5.1.6	La solution doit permettre d'attribuer une catégorie de sécurité à un projet.

C.4 SNC – Capacités du portail des partenaires et des policiers (P3)

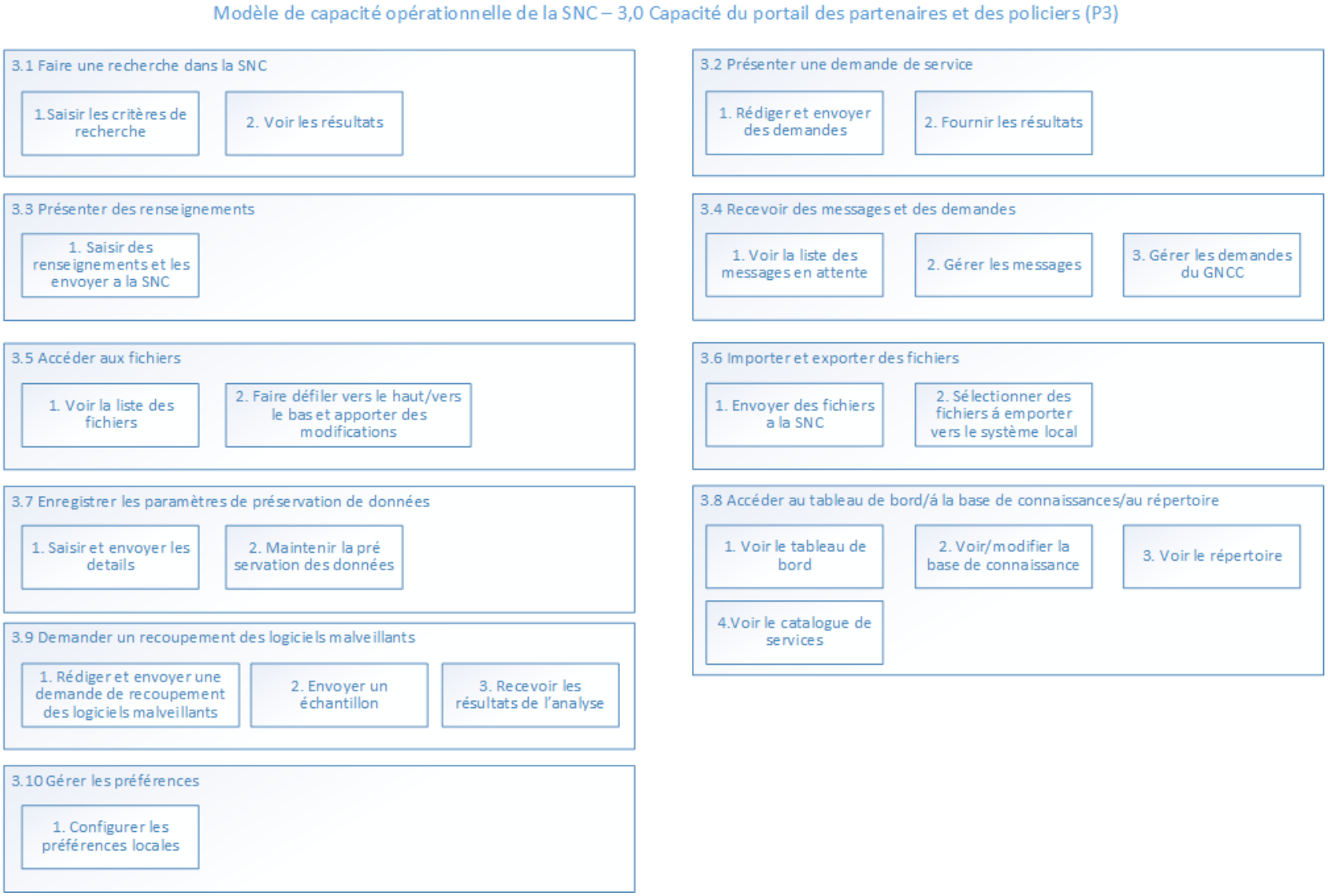


Figure C-4 : SNC – Capacités du P3

Tableau C-3 : SNC – Capacités du P3

3.1 Faire une recherche dans la SNC Permettre à un partenaire du P3 de faire une recherche dans la SNC et de recevoir les résultats de la recherche.	
3.1.1 Saisir les critères de recherche	
3.1.1.1	La solution doit permettre à l'utilisateur du P3 de saisir des critères de recherche, par exemple les suivants, sans s'y limiter : technique de recherche, motifs de la recherche, indicateur(s) de compromission, types de dossiers de la SNC (p. ex. préservation de données, plainte du public, cas soumis par un organisme d'application de la loi), endroits touchés par un cybercrime, dates limites, données cibles, émetteur des données.
3.1.1.2	La solution doit confirmer que les champs de recherche obligatoires sont remplis.
3.1.1.3	La solution doit être en mesure d'appliquer des techniques avancées de recherche, comme la correspondance parfaite, la recherche par proximité, les caractères de remplacement, les synonymes, la recherche d'expressions, les mots occultés et corrompus.
3.1.1.4	La solution doit permettre à l'utilisateur de sauvegarder une recherche - afin de pouvoir la choisir et la lancer de nouveau dans l'avenir.
3.1.1.5	La solution doit permettre à l'utilisateur de créer une liste de surveillance afin de déclencher l'envoi de messages si des recherches ou d'autres activités dans la SNC entraînent une correspondance avec du contenu figurant dans la liste de surveillance.
3.1.1.6	La solution doit permettre à l'utilisateur du P3 de mener une recherche dans tous les magasins de données de la SNC (p. ex. catalogues de données, bases de données objet, bases de données relationnelles) au moyen d'une seule recherche.
3.1.1.7	La solution doit permettre à l'utilisateur de mener une recherche en utilisant des critères, notamment en ce qui concerne les métadonnées, le type de contenu et le type de fichier.
3.1.2 Voir les résultats	
3.1.2.1	La solution doit montrer les résultats de la recherche à l'utilisateur du P3.
3.1.2.2	La solution doit fournir des renseignements comme les suivants, au minimum : l'émetteur des données, la date d'ajout à la SNC, le numéro du fichier, le numéro de cas de l'émetteur, le sommaire du fichier et les données correspondantes.
3.1.2.3	La solution doit fournir un classement relatif pour chaque rangée de résultats de recherche afin d'indiquer dans quelle mesure le résultat respecte les critères de la recherche.
3.2 Présenter une demande de service La solution doit être en mesure d'analyser l'information provenant des images ainsi que des zones de texte.	
3.2.1 Rédiger et envoyer des demandes	

Tableau C-3 : SNC – Capacités du P3

3.2.1.1	La solution doit permettre à l'utilisateur du P3 de créer une demande de service liée à des services comme les suivants (la liste doit être configurable) : a. Des demandes de recherche ponctuelles b. Une demande de recherche dans les bases de données des partenaires internationaux c. L'accès aux outils logiciels judiciaires et au bac à sable du GNCC d. Une demande de conseils et d'orientation techniques, d'aide dans le cadre d'une enquête ou d'autres renseignements e. Une demande d'analyse de renseignement f. L'ajout au répertoire des partenaires et à la base de connaissances g. Une demande pour une séance de clavardage sécurisé dans le P3 h. L'envoi d'une demande à un autre organisme du P3, ou la communication avec un tel organisme (communication et échange de renseignements entre les pairs) i. Autres - catégorie fourre-tout.
3.2.1.2	La solution doit faciliter la saisie, la validation et la transmission des renseignements nécessaires (selon le type de demande) aux fins de l'envoi d'une demande de service à la SNC. Par exemple, des listes déroulantes permettant de choisir le type de demande de service et des champs correspondants doivent être fournies pour aider l'utilisateur du P3 à remplir sa demande de service.
3.2.2 Fournir les résultats	
3.2.2.1	La solution doit fournir un accusé de réception ou les résultats à l'utilisateur du P3, selon le cas.
3.3 Présenter des renseignements Permettre au partenaire du P3 d'envoyer des données au GNCC afin que des correspondances puissent être établies avec le dépôt de données de la SNC et que les données puissent être ajoutées à celui-ci.	
3.3.1 Saisir des renseignements et les envoyer à la SNC	
3.3.1.1	La solution doit permettre à l'utilisateur du P3 de présenter des renseignements en matière de cybercriminalité au GNCC. Les renseignements peuvent notamment comprendre le numéro de cas, la désignation au titre du TLP, la désignation de sécurité, la date de péremption, les motifs de l'envoi, les indicateurs de compromission et les pièces jointes.
3.3.1.2	La solution doit permettre à l'utilisateur du P3 de joindre des pièces à son observation ou d'ajouter une pièce jointe à une observation déjà soumise.
3.3.1.3	La solution doit détecter si un fichier joint est trop volumineux et avertir l'utilisateur que la procédure de traitement des fichiers volumineux est requise.
3.3.1.4	La solution doit permettre à l'utilisateur du P3 de préciser la classification en matière d'échange de données (p. ex. TLP), la désignation de sécurité du gouvernement du Canada (p. ex. Protégé B) et la date de péremption qui sont associées à l'information soumise à la SNC.

Tableau C-3 : SNC – Capacités du P3

3.3.1.5	La solution doit permettre à l'utilisateur du P3 de créer un fichier de plainte du public ou de fraude en matière de cybercriminalité et de le soumettre aux fins de traitement.
3.4 Recevoir des messages et des demandes Permettre au partenaire du P3 d'accéder à des notifications en fonction de différents scénarios et permettre au GNCC de présenter des demandes au partenaire du P3. Les notifications et les demandes seront accessibles aux partenaires du P3 au moyen de la fonctionnalité du tableau de bord et des notifications.	
3.4.1 Voir la liste des messages en attente	
3.4.1.1	La solution doit fournir au partenaire du P3 un tableau de bord permettant de voir un résumé des messages ou des demandes provenant du GNCC ou d'autres organismes du P3.
3.4.1.2	La solution doit permettre à l'utilisateur du P3 de faire défiler vers le bas dans le résumé du tableau de bord pour voir la liste applicable des messages et des demandes, ainsi que les détails connexes, y compris les motifs du message, les détails relatifs à la demande et d'autres renseignements contextuels.
3.4.2 Gérer les messages	
3.4.2.1	La solution doit permettre à l'utilisateur du P3 d'ouvrir un message pour voir davantage de détails, comme le sujet, les organismes concernés, d'autres champs de données, les fichiers joints, les tâches ou les directives connexes.
3.4.2.2	La solution doit permettre à l'utilisateur du P3 de garder à jour le statut des messages et des demandes provenant du GNCC (p. ex. lu, non lu, en cours, mesure prise, fermé).
3.4.2.3	La solution doit permettre à l'utilisateur du P3 d'archiver et de cacher des messages.
3.4.3 Gérer les demandes du GNCC	
3.4.3.1	La solution doit permettre à l'utilisateur du P3 de voir les détails d'une demande du GNCC.
3.4.3.2	La solution doit faciliter la création d'une réponse de l'utilisateur du P3 en fournissant un modèle que l'utilisateur du P3 peut utiliser pour répondre à la demande du GNCC.
3.4.3.3	La solution doit établir un lien entre la réponse dans le P3 et le fichier pertinent dans la SNC.
3.5 Accéder aux fichiers Fournir aux partenaires du P3 un accès aux fichiers de plainte du public, aux billets et aux fichiers renvoyés par le GNCC (p. ex. trousse de renseignements permettant de prendre des mesures) qui ont été traités par le GNCC. Cet accès est fourni au moyen du sommaire du tableau de bord, l'utilisateur pouvant accéder à des listes d'éléments classés par catégorie à l'aide d'un défilement transversal.	
3.5.1 Voir la liste des fichiers	

Tableau C-3 : SNC – Capacités du P3

3.5.1.1	La solution doit fournir une liste par catégorie des billets et des fichiers de signalement public qui sont accessibles au partenaire du P3.
3.5.1.2	La solution doit fournir un tableau contenant de l'information indiquant le type de billet, de fichier ou de projet, la note et le degré de gravité établis par les responsables du triage et de l'évaluation du GNCC, ainsi que d'autres critères qui aideront le partenaire du P3 à établir l'ordre de priorité des éléments.
3.5.1.3	La solution doit permettre à l'utilisateur du P3 de gérer le statut du fichier dans sa file d'attente pour indiquer que des mesures ont été prises et pour préciser lesquelles.
3.5.1.4	La solution doit fournir une liste précise par catégorie des fichiers qui sont renvoyés à l'organisme en fonction de renseignements permettant la prise de mesures élaborés par le GNCC.
3.5.1.5	La solution doit permettre au partenaire du P3 de visualiser les fichiers de plainte du public selon les seuils configurables d'affichage des partenaires du P3.
3.5.1.6	La solution doit être en mesure de limiter l'accès de l'utilisateur du P3 aux fichiers en fonction d'un contrôle d'accès basé sur les rôles et d'un contrôle d'accès basé sur les attributs.
3.5.2 Faire défiler vers le haut et vers le bas et apporter des modifications	
3.5.2.1	La solution doit permettre à l'utilisateur de voir les détails de tout élément dans la file d'attente (p. ex. voir les détails du fichier, voir la trousse du renseignement) et de revenir à la file d'attente, au besoin.
3.5.2.2	La solution doit permettre à l'utilisateur du P3 de mettre le statut à jour ou d'ajouter des notes ou d'autres pièces jointes ou données requises (p. ex. le n° de cas dans le SGD local et les coordonnées de l'enquêteur) au billet, au fichier ou au projet auquel il accède.
3.5.2.3	La solution doit permettre à l'utilisateur du P3 de renvoyer un billet, un fichier ou un projet à un autre service de police ou de signaler au GNCC qu'il ne peut pas procéder à un renvoi.
3.5.2.4	La solution doit permettre à l'utilisateur du P3 d'accéder à la fonctionnalité applicable d'analyse de données qui est offerte aux utilisateurs du GNCC.
3.6 Importer et exporter des fichiers Fournir au partenaire du P3 la capacité de choisir un fichier à partir d'une liste du P3 et de l'importer dans son SGD local. Cette fonctionnalité entraînera la création d'un fichier sous un format qui peut être importé dans le SGD local. Cette capacité permet également au partenaire du P3 de choisir un fichier local et de l'exporter vers la SNC. Les formats de fichier doivent respecter une norme prédéterminée pour l'échange de données entre le SGD et la SNC. Veuillez noter que l'utilisation de cette fonctionnalité exige que le SGD local ait la capacité d'importer un fichier structuré ou de créer un fichier structuré à partir d'un fichier de cas afin qu'il soit transmis à la SNC. Veuillez également noter que cette interface a été décrite selon les exigences relativement courantes. Au besoin, les considérations liées à la conception et à la mise en œuvre peuvent l'emporter sur la description fournie.	
3.6.1 Envoyer des fichiers à la SNC	

Tableau C-3 : SNC – Capacités du P3

3.6.1.1	La solution doit permettre à l'utilisateur du P3 de choisir un fichier formaté (conformément aux normes d'échange de données prescrites du GNCC) et de l'envoyer au GNCC.
3.6.2 Sélectionner des fichiers à importer vers le système local	
3.6.2.1	La solution doit permettre à l'utilisateur du P3 de choisir un fichier dans sa liste des travaux en attente et d'indiquer qu'il souhaite l'importer dans son SGD local.
3.6.2.2	La solution doit créer un fichier selon la norme convenue pour l'échange de données et sauvegarder le fichier dans le système local, où il peut être par la suite intégré par le SGD local, qui crée un fichier de cas (en supposant que le SGD a la capacité d'intégrer ces fichiers - conformément à une norme convenue).
3.7 Enregistrer les paramètres de préservation des données L'utilisateur du P3 peut saisir les détails d'une demande ou d'une ordonnance de préservation des données qu'il exécute contre un consignataire local de données et envoyer ces détails à la SNC. La SNC établira les correspondances avec le dépôt de la SNC à des fins d'élimination des conflits.	
3.7.1 Saisir et envoyer les détails	
3.7.1.1	La solution doit permettre à l'utilisateur du P3 de saisir les détails (comme : données étrangères ou nationales, l'objet de la préservation des données, les données qui doivent être préservées, les coordonnées du consignataire de données, les dates applicables, le numéro local du cas et les coordonnées) associés à la demande ou à l'ordonnance de préservation des données qu'il exécute à l'égard d'un consignataire de données au Canada ou au titre de laquelle il présente une demande à l'international.
3.7.2 Maintenir la préservation des données	
3.7.2.1	La solution doit permettre à l'utilisateur du P3 de voir les demandes et les ordonnances de préservation des données qu'il a enregistrées.
3.7.2.2	La solution doit permettre à l'utilisateur du P3 de signaler que la demande ou l'ordonnance de préservation des données est annulée, qu'elle a été renouvelée (avec les dates applicables) ou qu'elle a mené à une ordonnance de communication.
3.8 Accéder au tableau de bord, à la base de connaissances et au répertoire Le tableau de bord du P3 contiendra un résumé des renvois et d'autres renseignements relatifs à la compétence. Il fournira un point de départ à partir duquel l'utilisateur du P3 peut naviguer pour consulter les listes des travaux en attente ou bien des demandes, messages, rapports et renvois particuliers, au besoin.	
3.8.1 Voir le tableau de bord	
3.8.1.1	La solution doit permettre à l'utilisateur du P3 de voir un tableau de bord qui présente des renseignements et des graphiques généraux et d'accéder aux demandes, messages, rapports statistiques, renvois ou autres détails pertinents grâce à un défilement transversal.

Tableau C-3 : SNC – Capacités du P3

3.8.1.2	La solution doit comprendre des statistiques sur l'administration locale, y compris des tendances, des représentations géographiques et des cartes thermiques, lesquelles sont affichées dans le tableau de bord du P3.
3.8.1.3	La solution doit permettre à l'utilisateur de personnaliser le contenu de son tableau de bord en choisissant des éléments de contenu prédéfinis (p. ex. « tuiles »).
3.8.2 Voir et modifier la base de connaissances	
3.8.2.1	La solution doit permettre à l'utilisateur du P3 de consulter, d'interroger, de trouver et de visionner une bibliothèque de contenu et de liens menant vers des ressources éducatives et des outils de travail; des listes de vérification destinées aux agents de réception de première ligne; des modèles; des lignes directrices; des scénarios; des conseils; des précédents; de la jurisprudence.
3.8.2.2	La solution doit permettre à l'utilisateur du P3 d'ajouter des documents à la base de connaissances. Veuillez noter que ce contenu sera d'abord approuvé aux fins de publication par le GNCC.
3.8.2.3	La solution doit permettre à l'utilisateur de télécharger et d'imprimer les documents et les fichiers accessibles par l'entremise de la base de connaissances.
3.8.3 Voir le répertoire des partenaires	
3.8.3.1	La solution doit fournir aux utilisateurs du P3 un répertoire interrogeable des ressources (p. ex. personnes et organisations), comme les fournisseurs d'accès à Internet, les entreprises faisant l'échange de devises numériques, les personnes-ressources en matière de sécurité des TI, les experts en matière de cybercriminalité provenant d'organismes d'application de la loi, les enquêteurs en matière de cybercriminalité et de fraude (NCFTA, CCCS, GRC, FBI Internet Crime Complaint Centre, Centre européen de lutte contre la cybercriminalité).
3.8.4 Voir le catalogue de services	
3.8.4.1	La solution doit permettre à l'utilisateur de consulter, d'interroger, de trouver et de voir les outils logiciels offerts par l'entremise « de la boîte à outils et du bac à sable » en matière de cybercriminalité du GNCC.
3.8.4.2	La solution doit permettre à l'utilisateur de demander l'accès à des outils et de prévoir une période d'accès au bac à sable du GNCC. Veuillez noter que le « bac à sable » est extensible, de sorte que l'accès à cet espace ne devrait pas poser problème.
3.9 Demander un recoupement des logiciels malveillants Permettre au partenaire du P3 de demander que le GNCC effectue un recoupement ou une analyse d'un logiciel malveillant. La solution permettra à l'utilisateur du P3 de soumettre un échantillon d'un logiciel malveillant ou l'algorithme de hachage d'un logiciel malveillant aux fins de recoupement et d'analyse.	
3.9.1 Rédiger et envoyer une demande de recoupement des logiciels malveillants	
3.9.1.1	La solution doit permettre à l'utilisateur du P3 de saisir les détails de sa demande de recoupement d'un logiciel malveillant (p. ex. n° du fichier local, contexte, échantillon du logiciel malveillant pour soumettre un indicateur, aux fins de renseignement seulement,

Tableau C-3 : SNC – Capacités du P3

	lié à une enquête en cours, conclusions seront utilisées dans le cadre d'une communication préalable) et d'envoyer la demande à la SNC.
3.9.2 Envoyer un échantillon	
3.9.2.1	La solution doit permettre à l'utilisateur du P3 de soumettre son échantillon de logiciel malveillant.
3.9.2.2	La solution doit comprimer, condenser et isoler de façon sécuritaire les échantillons de logiciels malveillants des autres données de la GRC.
3.9.3 Recevoir les résultats de l'analyse	
3.9.3.1	La solution doit renvoyer un message indiquant que l'analyse du logiciel malveillant est terminée au moyen du tableau de bord du P3.
3.9.3.2	La solution doit permettre à l'utilisateur du P3 d'accéder aux résultats de l'analyse du logiciel malveillant.
3.10 Gérer les préférences Permettre à l'utilisateur autorisé du P3 (selon le contrôle d'accès en fonction des rôles) de gérer les préférences du système du P3 pour l'organisme du P3.	
3.10.1 Configurer les préférences locales	
3.10.1.1	La solution doit permettre à l'utilisateur autorisé du P3 de choisir différents paramètres de configuration qui sont propres à l'utilisation du P3 par l'organisme. Voici certains exemples : envoi d'un courriel à l'échelle locale en cas d'alerte, options de notification (p. ex. chaque heure, chaque jour, chaque semaine) et coordonnées.
3.10.1.2	La solution doit permettre à l'utilisateur du P3 de voir et de gérer une liste des indicateurs de compromission (liste de surveillance) qui présentent un intérêt particulier pour l'organisation de cet utilisateur
3.10.1.3	La solution doit permettre à l'utilisateur du P3 d'établir des paramètres relatifs au seuil de signalement public afin de séparer les signalements publics permettant de prendre des mesures des signalements présentant une faible valeur.

C.5 SNC – CAPACITÉS DES SERVICES FONCTIONNELS

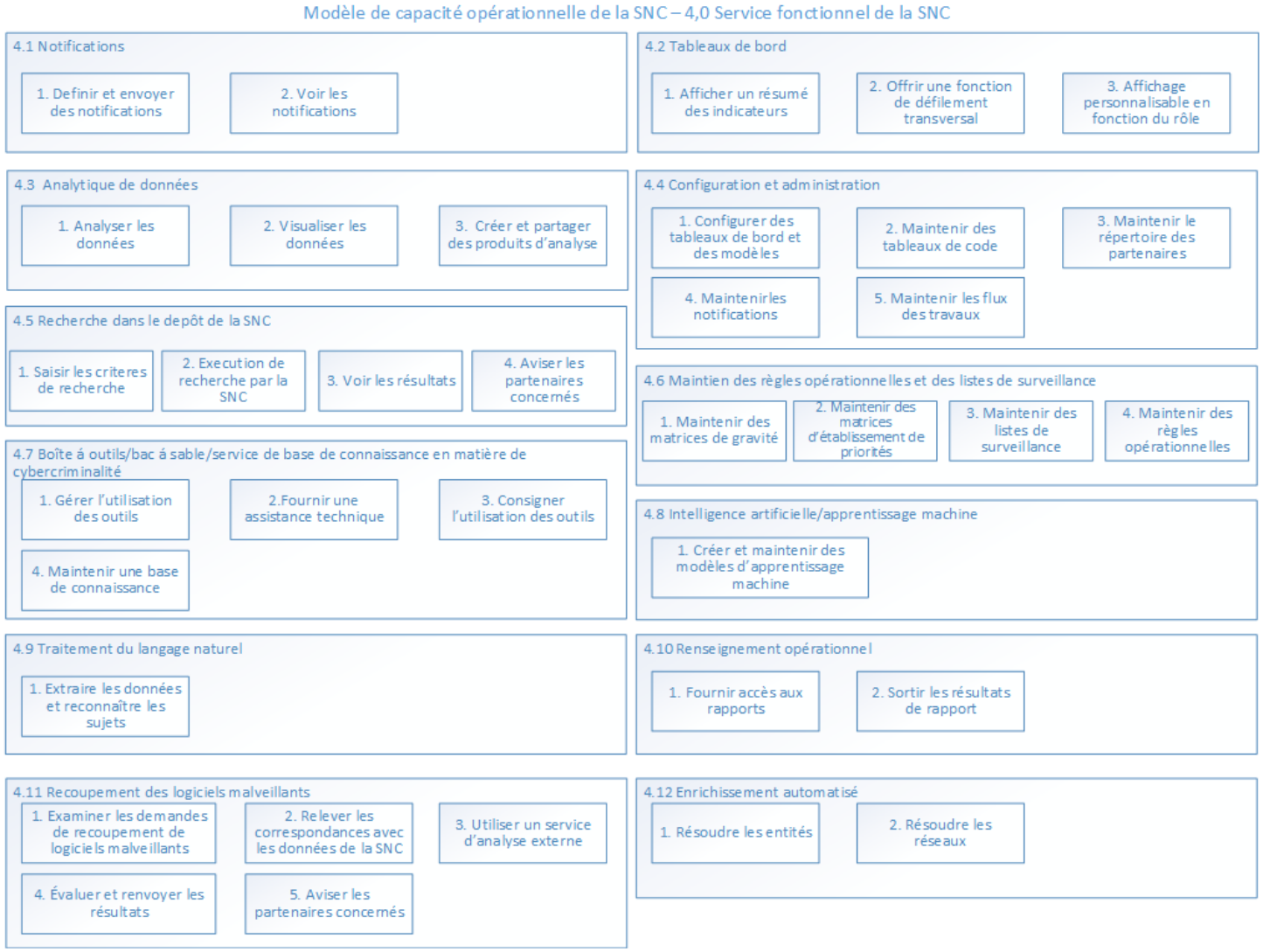


Figure C-5 : SNC – Capacités des services fonctionnels

Tableau C-4 : SNC — Capacités des services fonctionnels

4.1 Notifications Certains événements qui surviennent dans la solution, comme une correspondance entre des données, l'attribution d'une tâche ou l'atteinte d'une date de péremption, entraîneront l'envoi d'une notification aux parties concernées. La solution doit tenir compte des règles de divulgation pour acheminer les notifications. La solution doit également afficher et gérer les notifications pour les utilisateurs concernés. Les événements qui déclenchent l'envoi d'une notification sont documentés sous la forme de capacités dans d'autres sections appropriées du modèle de capacité. Par exemple, des notifications sont envoyées lorsqu'une correspondance est établie entre des données et certaines entités, notamment des indicateurs de compromission, des listes de surveillance, des critères de recherche utilisés dans le passé, des activités de préservation des données, des travaux que mène actuellement la Section du renseignement ou la Section de la coordination opérationnelle du GNCC à l'égard d'un fichier ou des analyses de données connexes, ou encore lorsque des données sont ajoutées au dépôt, que des demandes de préservation des données sont présentées ou que d'autres activités d'enrichissement sont menées.	
4.1.1 Définir et envoyer les notifications	
4.1.1.1	La solution doit envoyer automatiquement des notifications aux utilisateurs, aux groupes, aux organismes d'application de la loi ou aux partenaires en matière de cybercriminalité concernés en fonction des différents déclencheurs propres à l'utilisateur ou au système, définis dans l'ensemble de la solution.
4.1.1.2	La solution doit tenir compte de toutes les limites en matière de divulgation, y compris la désignation au titre du TLP et les désignations en matière de sécurité des données, au moment de présenter une notification ou des données. Par exemple, une notification, un message ou des données affichées peuvent être modifiés pour inclure seulement de l'information sous la forme de pointeurs (liens) lorsque la désignation au titre du TLP restreint le partage ou que la désignation de sécurité des données dépasse l'autorisation du destinataire.
4.1.1.3	La solution doit permettre à un analyste du GNCC d'envoyer manuellement une notification à un utilisateur, à un groupe, à un organisme d'application de la loi ou à un partenaire en matière de cybercriminalité. Le contenu des notifications envoyées manuellement est également assujetti aux limites en matière de divulgation.
4.1.1.4	La solution doit enregistrer automatiquement toutes les notifications envoyées - peu importe le mode d'envoi et le type de notification.
4.1.1.5	La solution doit fournir, par courriel, des notifications sur le P3 aux partenaires en matière de cybercriminalité et aux organismes d'application de la loi; le courriel mentionnera que les détails sont disponibles dans le P3.
4.1.1.6	La solution doit aviser l'utilisateur du GNCC si une notification ne peut pas être envoyée en raison d'un avertissement en matière d'échange de données ou d'une autre règle opérationnelle.
4.1.1.7	La solution doit être en mesure d'envoyer des notifications par courriel et sous la forme de texte (comme défini dans le profil des notifications) à un ou plusieurs utilisateurs cibles configurables, parallèlement à une notification sur le P3. Cela vise à permettre le traitement des notifications à l'extérieur des heures ouvrables, dans certaines situations hautement prioritaires.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.1.1.8	La solution doit permettre aux utilisateurs de configurer les règles opérationnelles en matière de correspondance afin de gérer le volume de notifications.
4.1.2 Voir les notifications	
4.1.2.1	La solution doit permettre à l'utilisateur de voir les notifications qui lui ont été envoyées.
4.1.2.2	La solution doit permettre à l'utilisateur de filtrer, de trier et d'archiver les notifications et de faire une recherche pour retrouver des notifications précises ou afficher les notifications de certains types.
4.1.2.3	La solution doit permettre à l'utilisateur de faire défiler vers le bas au moment d'afficher une notification afin de voir le fichier ou le billet sous-jacent ainsi que toute autre entité liée à la notification.
4.2 Tableaux de bord Les tableaux de bord seront utilisés pour fournir un résumé des renseignements importants selon le rôle de l'utilisateur. Le tableau de bord peut permettre à l'utilisateur de procéder à un défilement transversal pour atteindre des listes détaillées de tâches ou de travaux en attente, afin d'accéder à ses tâches quotidiennes. Dans le cas des gestionnaires, les tableaux de bord doivent fournir un sommaire des indicateurs opérationnels, ce qui leur permettra de connaître en temps réel l'état des activités du GNCC.	
4.2.1 Afficher un résumé des indicateurs	
4.2.1.1	La solution doit fournir des tableaux de bord contenant des tuiles qui affichent des visualisations graphiques de données regroupées, notamment en ce qui concerne les demandes de service, les observations et les travaux opérationnels en cours du GNCC.
4.2.1.2	La solution doit permettre aux utilisateurs du GNCC de voir des résumés des données actuelles sous la forme de graphiques et de tableaux, lesquels contiennent des indicateurs clés de rendement relativement à des activités liées aux flux des travaux, notamment les suivantes : a. réception; b. triage; c. évaluation; d. analyse de données; e. coordination des renseignements; f. coordination opérationnelle.
4.2.1.3	La solution doit permettre aux utilisateurs autorisés du GNCC et du P3 de visualiser des graphiques standards contenant des résumés établis en temps quasi réel des données intégrées au dépôt de données de la SNC. Un tableau de bord pourrait notamment comprendre : a. des cartes thématiques sur les écarts statistiques; b. des statistiques sur la fraude et la cybercriminalité à l'échelle régionale, locale et nationale; c. les volumes de demandes, les correspondances trouvées; d. les volumes de cas en cours, selon le statut; e. des tableaux des tendances

Tableau C-4 : SNC — Capacités des services fonctionnels

4.2.2 Offrir une fonction de défilement transversal, au besoin	
4.2.2.1	La solution doit permettre à l'utilisateur de faire défiler les éléments vers le bas (et vers le haut) dans le tableau de bord pour afficher une liste ou d'autres représentations détaillées des entités de données qui contribuent au graphique ou à la représentation statistique choisi dans le tableau de bord.
4.2.3 Affichage personnalisable en fonction du rôle	
4.2.3.1	La solution doit permettre à l'utilisateur de personnaliser l'affichage standard de son tableau de bord et de sauvegarder ses paramètres en tant qu'affichage du tableau de bord propre à l'utilisateur. Cela comprend, sans s'y limiter, la capacité de choisir quelles tuiles doivent figurer dans le tableau de bord.
4.3 Analytique de données Les capacités d'analytique de données permettront de créer des renseignements ou des données utiles à partir de texte brut ou d'images. Le GNCC intégrera les données provenant de plusieurs sources, lesquelles seront transformées au besoin et analysées au moyen d'outils d'analyse du renseignement en matière criminelle. Les renseignements générés seront utilisés pour orienter la prise de décisions et produire des renseignements permettant aux organismes d'application de la loi de prendre des mesures.	
4.3.1 Analyser les données	
4.3.1.1	La solution doit permettre d'effectuer une analyse approfondie des données dans le dépôt de données de la SNC; de visualiser les données (p. ex. les données brutes, les données nettoyées, les résultats de l'exécution d'un code, les résultats des modèles); et d'exporter ou d'associer des modèles, des extrants et des projets d'analyse afin de les communiquer aux utilisateurs du P3.
4.3.1.2	La solution doit permettre à l'utilisateur de travailler dans un environnement de science des données interactif et collaboratif afin de manipuler les données, le code et les modèles associés à un fichier, ainsi que parallèlement à d'autres sources de données; de stocker temporairement des données, de nettoyer et de transformer des données; de construire des modèles d'analyse, d'écrire du code, d'exécuter du code, en tout ou en partie; d'effectuer le contrôle des versions pour les projets d'analyse et les fichiers connexes; d'associer des fichiers, des projets et les données et modèles qu'ils contiennent et de les communiquer à d'autres utilisateurs; de visualiser les données (p. ex. les données brutes, les données nettoyées, les résultats de l'exécution d'un code, les résultats des modèles); et d'exporter ou d'associer des modèles, des extrants et des projets d'analyse afin de les communiquer aux utilisateurs du P3.
4.3.1.3	La solution doit fournir aux utilisateurs les outils permettant d'automatiser la collecte de renseignements provenant de sources ouvertes. Les outils de renseignement de sources ouvertes devraient faciliter l'identification des entités (p. ex. les entreprises, les victimes ou les victimes potentielles, les adresses physiques, les suspects potentiels), à l'aide de différents critères, comme des noms d'entreprises, des adresses physiques, des adresses IP et des adresses Web.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.3.2 Visualiser les données	
4.3.2.1	La solution doit permettre de produire et d'afficher des tableaux et des diagrammes, notamment sous les formes suivantes : diagrammes de liens, organigrammes, diagrammes d'événements, cartes géospatiales et autres représentations graphiques établis à partir des données enrichies par l'outil d'analyse.
4.3.2.2	La solution doit permettre de sauvegarder le texte, les diagrammes et les images graphiques du produit de renseignement sous un format de fichier pouvant être exporté, comme un PDF (Adobe Acrobat).
4.3.2.3	La solution doit permettre à l'utilisateur de créer des produits de renseignement exhaustifs contenant des données sélectionnées sous la forme de texte et de représentations graphiques.
4.3.2.4	La solution doit permettre à l'analyste de renseignements d'appliquer la désignation au titre du TLP et de caviarder les trousses et produits de renseignement ou les autres renseignements diffusés.
4.3.2.5	La solution doit permettre aux utilisateurs de visualiser et d'imprimer des rapports d'analyse (p. ex. des produits de renseignement).
4.3.3 Créer et partager des produits d'analyse	
4.3.3.1	La solution doit permettre à l'analyste de créer des rapports d'analyse, des extrants ou des renseignements connexes (p. ex. connaissance de la situation, notification des victimes, résultats d'analyse, partiels ou finaux) et de partager ces produits avec des organismes et utilisateurs choisis par l'entremise du P3, par courriel ou au moyen d'un autre portail sécurisé.
4.3.3.2	La solution doit permettre à l'analyste d'ajouter des filigranes configurables (p. ex. « Confidentiel », « La règle relative aux tiers s'applique », « Protégé B ») aux rapports d'analyse.
4.3.3.3	La solution doit permettre à l'utilisateur de caviarder (cacher ou retenir des renseignements qui ne peuvent être divulgués) de façon sélective des champs de renseignements précis ou du texte libre pour protéger les sources ou les autres personnes identifiables qui ne sont pas le sujet du fichier.
4.3.3.4	La solution doit permettre à l'utilisateur de créer et de joindre des valeurs de hachage relativement aux rapports et pièces jointes, lesquelles peuvent être distribuées avec le rapport ou la pièce jointe.
4.3.3.5	La solution doit permettre l'examen et l'approbation des rapports, des notifications et d'autres extrants (par les utilisateurs autorisés du GNCC) avant la distribution.
4.3.3.6	La solution doit permettre à l'utilisateur de diffuser des rapports approuvés, comme des notifications aux victimes, directement à une victime ou à une victime potentielle.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.4 Configuration et administration Les capacités de configuration et d'administration de la SNC comprennent une fonctionnalité permettant de gérer la configuration et la maintenance du système. Cette capacité englobe, sans s'y limiter, la gestion des comptes d'utilisateur, des tableaux de code, des tuiles des tableaux de bord, des renseignements sur les partenaires, des clés publiques et d'autres paramètres du système.	
4.4.1 Configurer des tableaux de bord et des modèles	
4.4.1.1	La solution doit permettre à l'utilisateur autorisé du GNCC de gérer les affichages standards du tableau de bord ou le contenu de celui-ci en créant, en modifiant ou en supprimant des tuiles qui peuvent être sauvegardées et consultées par l'utilisateur.
4.4.2 Maintenir des tableaux de code et du contenu d'aide	
4.4.2.1	La solution doit permettre à l'utilisateur autorisé de gérer le contenu des tableaux de code utilisés pour la validation des entrées encodées et l'affichage des listes déroulantes dans l'interface de l'utilisateur.
4.4.2.2	La solution doit permettre à l'utilisateur autorisé du GNCC de gérer le contenu d'aide en ligne.
4.4.3 Maintenir le répertoire des partenaires	
4.4.3.1	La solution doit permettre à l'utilisateur autorisé de gérer les renseignements figurant au profil des partenaires du GNCC en matière de cybercriminalité, des organismes d'application de la loi et de tous les autres intervenants avec lesquels le GNCC interagit. Les profils comprennent de l'information comme le type de partenaire, les coordonnées, le niveau d'expertise en cybercriminalité, les coordonnées et la procédure pour la transmission d'un dossier aux paliers supérieurs.
4.4.3.2	La solution doit permettre à l'utilisateur autorisé du GNCC de gérer les préférences, les seuils et les règles relatifs aux renvois ainsi que les relations hiérarchiques entre les organismes d'application de la loi aux fins des renvois.
4.4.3.3	La solution doit permettre d'associer et de maintenir des attributs afin d'aider à identifier le service de police compétent. Les attributs peuvent comprendre l'emplacement géographique, l'adresse municipale, l'adresse postale (code postal) et l'adresse IP.
4.4.3.4	La solution doit donner aux utilisateurs potentiels un moyen de soumettre des demandes d'accès en ligne à la SNC (y compris le P3).
4.4.3.5	La solution doit permettre aux utilisateurs autorisés d'examiner, d'approuver et de lancer les procédures d'intégration liées aux demandes de comptes d'utilisateur.
4.4.4 Maintenir les notifications	
4.4.4.1	La solution doit permettre à l'utilisateur autorisé de créer, de modifier ou de retirer des modèles de notification.
4.4.4.2	La solution doit permettre à l'utilisateur autorisé de gérer les règles au titre desquelles une notification doit être envoyée et de choisir quel modèle doit être utilisé.
4.4.4.3	La solution doit permettre à l'utilisateur autorisé de préciser, au moyen d'un modèle de notification et d'un critère relatif à la règle opérationnelle, qu'un courriel et un message texte doivent également être envoyés au destinataire de la notification.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.4.5 Maintenir les flux des travaux	
4.4.5.1	La solution doit permettre à l'utilisateur autorisé du GNCC de créer, de modifier ou de retirer des flux des travaux. Cela comprend, sans s'y limiter, la création automatique de tâches et l'attribution automatique de tâches ou de fichiers à des utilisateurs ou à des groupes.
4.4.5.2	La solution doit permettre à l'utilisateur autorisé du GNCC de gérer les modèles standards que les utilisateurs du P3 utilisent pour soumettre des observations structurées et des demandes de service.
4.5 Recherche dans le dépôt de la SNC Les capacités de recherche dans le dépôt de la SNC permettront aux utilisateurs (GNCC et P3) d'interroger un magasin central de renseignements liés à la cybercriminalité à l'aide de techniques avancées tenant compte des aspects propres à la cybercriminalité des données. Les recherches dans la SNC permettront également de déclencher l'envoi de notifications relatives à l'établissement d'une correspondance lorsqu'un intérêt mutuel est découvert par l'entremise des résultats de la recherche ou de l'utilisation des mêmes paramètres de recherche.	
4.5.1 Saisir les critères de recherche	
4.5.1.1	La solution doit permettre de faire une recherche dans l'ensemble ou une partie du contenu du dépôt de données de la SNC. Par exemple, les limites au chapitre de la date, de la zone géographique ou du type de crime peuvent être utilisées en tant que paramètres.
4.5.1.2	La solution doit offrir des méthodes flexibles de recherche des correspondances, y compris, sans s'y limiter : a. correspondance exacte d'un mot ou d'une expression; b. recherches par proximité; recherches de mots précis qui sont espacés d'un certain nombre de mots; c. recherches par proximité au sein de phrases ou de paragraphes; d. recherches avec caractères de remplacement; e. recherches à l'aide des opérateurs booléens; f. synonymes des mots précisés dans les critères de recherche; g. recherche approximative (p. ex. Soundex) h. mots occultés (p. ex. pirate = p1r4t3, captain = c4pt41n, disco = d1$c0, mysite.com = mysite dot com); i. toute combinaison des critères de recherche mentionnés plus haut dans le cadre de la même recherche.
4.5.1.3	La solution doit, pour tous les utilisateurs du GNCC et du P3, offrir une interface d'interrogation en langage naturel et une interface utilisateur à base de formulaires afin d'aider l'utilisateur à définir les critères d'une recherche.
4.5.1.4	La solution doit permettre à l'utilisateur de sauvegarder les critères de recherche pour les réutiliser lors d'une interrogation future.
4.5.1.5	La solution doit permettre à l'utilisateur de préciser que la recherche doit être silencieuse. Les résultats d'une telle recherche sont renvoyés seulement à l'organisme qui a effectué la recherche. La recherche silencieuse ne déclenchera pas l'envoi d'une notification relative à l'utilisation des mêmes critères de recherche. Veuillez noter que cette fonctionnalité ne l'emportera pas sur les paramètres relatifs à l'envoi de notifications aux utilisateurs du GNCC. Cette option s'appliquera uniquement aux notifications envoyées aux organismes externes d'application de la loi et aux partenaires.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.5.1.6	La solution doit faire une recherche dans l'historique de recherche afin de relever les recherches semblables et fournir une réponse pour indiquer si d'autres utilisateurs ont utilisé les mêmes critères ou des critères semblables dans le passé.
4.5.1.7	La solution doit permettre à l'utilisateur de faire une recherche dans les champs ou les attributs applicables du dépôt de la SNC, y compris, sans s'y limiter, les indicateurs de compromission, les valeurs de hachage, les outils, les techniques et les procédures, les attributs des billets, des fichiers ou des projets, y compris les zones de texte libre.
4.5.1.8	Par défaut, la solution doit, si plus d'un critère est utilisé, fournir les résultats qui correspondent à l'ensemble des critères (selon la méthode de recherche choisie) et permettre à l'utilisateur de passer outre à cette fonctionnalité et d'obtenir les résultats qui correspondent à n'importe lequel des critères.
4.5.1.9	La solution doit permettre à l'utilisateur d'effectuer une recherche fédérée dans l'ensemble des magasins de données de la SNC (p. ex. données recueillies durant la période initiale de capacité opérationnelle, catalogues de données, bases de données objet, bases de données relationnelles) au moyen d'une seule recherche.
4.5.1.10	La solution doit permettre à l'utilisateur de préciser une cote minimale pour sa recherche - ou une cote minimale pour une recherche effectuée automatiquement. Les résultats qui n'atteignent pas la cote minimale ne seront pas affichés.
4.5.2 Exécution de la recherche par la SNC	
4.5.2.1	La solution doit être en mesure de mener une recherche dans le dépôt de la SNC à l'aide des critères précisés par l'utilisateur.
4.5.2.2	La solution doit appliquer les règles relatives au contrôle d'accès basées sur les rôles (RBAC) et au contrôle d'accès basé sur les attributs (ABAC) (p. ex. TLP, désignation de sécurité de l'information) afin de faire une recherche dans les résultats pour établir quelles données peuvent être renvoyées à l'utilisateur.
4.5.2.3	La solution doit, dans le cas des données qui ont été jugées comme ne pouvant pas être divulguées, préciser dans les résultats de la recherche que des renseignements supplémentaires sont disponibles et fournir les coordonnées de l'émetteur des données.
4.5.2.4	La solution doit générer une cote pour chaque résultat qui est renvoyé à l'utilisateur en fonction du degré de correspondance avec les critères de recherche.
4.5.2.5	La solution doit montrer à l'utilisateur qui a fait la recherche, en plus des résultats, la cote de correspondance, le type de correspondance trouvée (p. ex. une correspondance avec une ancienne recherche, une demande de préservation des données, une divulgation de données, un fichier de plainte) et d'autres données sommaires.
4.5.2.6	La solution doit être capable d'effectuer des recherches multilingues afin d'extraire des résultats stockés dans une langue différente que les critères de recherche.
4.5.3 Voir les résultats	
4.5.3.1	La solution doit permettre à l'utilisateur de voir les résultats de la recherche.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.5.3.2	La solution doit permettre à l'utilisateur de filtrer et de trier toutes les colonnes de données présentées au moment d'afficher les résultats. L'ordre par défaut doit tenir compte du contexte de la recherche; des facteurs comme la cote obtenue, la date ou l'ordre alphabétique peuvent être utilisés comme ordre par défaut.
4.5.3.3	La solution doit permettre à l'utilisateur de faire défiler vers le bas dans toute rangée de résultats sélectionnée afin de voir les détails des données pour lesquelles une correspondance a été établie (p. ex. ouvrir le fichier, la demande de préservation des données en question et faire défiler vers le haut pour revenir aux résultats).
4.5.3.4	La solution doit permettre à l'utilisateur d'imprimer ou de sauvegarder les résultats d'une recherche.
4.5.3.5	La solution doit mettre en surbrillance les termes recherchés dans les résultats et les documents applicables (option configurable).
4.5.4. Aviser les parties concernées	
4.5.4.1	La solution doit envoyer les notifications requises si elle découvre une corrélation avec le dépôt du GNCC ou avec une recherche semblable précédemment effectuée. Si l'indicateur de recherche silencieuse est activé, le comportement doit être modifié de façon à ce que seules les notifications à la SNC soient envoyées.
4.5.4.2	La solution doit comporter une fonctionnalité de correspondance sans intervention. Si une correspondance est établie avec des données existantes liées à un indicateur de correspondance sans intervention, les données ne doivent pas figurer dans les résultats, mais l'organisme qui a fourni les données doit être avisé. Les correspondances avec l'historique de recherche seront renvoyées à l'utilisateur.
4.6 Maintenir les règles opérationnelles et les listes de surveillance Les règles opérationnelles serviront à établir le degré de gravité des observations reçues par le GNCC. De plus, les règles opérationnelles serviront à cerner les observations qui présentent un intérêt pour différentes sections de la SNC. Lorsqu'on découvre une observation présentant un intérêt, la section concernée du GNCC sera avisée.	
4.6.1 Maintenir des matrices de gravité	
4.6.1.1	La solution doit permettre à l'utilisateur autorisé de définir les règles opérationnelles nécessaires à l'attribution d'une cote de gravité pour chaque demande de service, observation et plainte du public intégrée par la solution.
4.6.2 Maintenir des matrices d'établissement des priorités	
4.6.2.1	La solution doit permettre à l'utilisateur autorisé de définir les règles opérationnelles (matrices d'établissement des priorités) qui permettront de cerner les observations présentant un intérêt pour une section précise du GNCC, p. ex. la Section du renseignement ou la Section de la coordination opérationnelle. Les sections peuvent définir leurs propres règles opérationnelles.
4.6.2.2	La solution doit permettre à l'utilisateur autorisé de modifier les règles et les seuils pour chaque matrice d'établissement des priorités définie.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.6.3 Maintenir des listes de surveillance	
4.6.3.1	La solution doit permettre à l'utilisateur du GNCC de gérer des listes de surveillance d'indicateurs de compromission, de tactiques, techniques et procédures (TTP) ou d'autres entités présentant un intérêt précis pour une section du GNCC.
4.6.3.2	La solution doit permettre la création de listes de surveillance pour différentes sections du GNCC.
4.6.4. Maintenir des règles opérationnelles	
4.6.4.1	La solution doit permettre à l'utilisateur autorisé de configurer les règles opérationnelles qui gouvernent les activités, comme les flux des travaux du système.
4.6.4.2	La solution doit permettre à l'utilisateur autorisé du GNCC de mettre en place ou de retirer un indicateur de correspondance sans intervention pour le GNCC, ou de passer outre à un tel indicateur (de façon temporaire ou permanente). Veuillez noter qu'il peut être demandé au GNCC d'établir un indicateur de correspondance sans intervention à l'égard de certaines données, ou le Groupe peut avoir à passer outre à ces indicateurs pour obtenir une connaissance de la situation, afin de pouvoir soutenir la coordination opérationnelle.
4.7 Boîte à outils, bac à sable et service de base de connaissances en matière de cybercriminalité Le GNCC offrira un service aux organismes canadiens d'application de la loi qui permettra aux services de police d'utiliser des applications logicielles judiciaires liées à la cybercriminalité. En outre, le GNCC offrira un « bac à sable » dans lequel les organismes peuvent analyser les données au moyen de ces outils, tout en profitant de la capacité d'établir des correspondances avec le dépôt de données sur la cybercriminalité de la SNC, ainsi que de verser les résultats dans le dépôt. De plus, les capacités du GNCC de maintenir la base de connaissances fournie par l'entremise du P3 sont décrites ici.	
4.7.1 Gérer l'utilisation des outils	
4.7.1.1	La solution doit être en mesure de gérer les demandes d'utilisation des applications et des services judiciaires en matière de cybercriminalité qui sont offerts par le GNCC.
4.7.2 Fournir une assistance technique	
4.7.2.1	La solution doit permettre aux ressources du GNCC de faire le suivi des activités liées à la prestation d'une assistance aux organismes d'application de la loi quant à la configuration et à l'utilisation des outils.
4.7.3 Consigner l'utilisation des outils	
4.7.3.1	La solution doit être en mesure d'incorporer les résultats des outils d'analyse judiciaire dans le dépôt de la SNC aux fins de l'établissement de correspondances, de l'élimination des conflits et de la connaissance de la situation.
4.7.3.2	La solution doit être en mesure d'aviser les utilisateurs du GNCC lorsque des correspondances sont établies au moyen des résultats découlant de l'utilisation des outils dans le bac à sable.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.7.4 Maintenir une base de connaissances	
4.7.4.1	La solution doit permettre aux utilisateurs de gérer le contenu de la base de connaissances qui est offert aux utilisateurs du P3 et qui figure sur le site Web du portail public.
4.7.4.2	La solution doit permettre aux utilisateurs de maintenir un catalogue des services offerts par le GNCC.
4.7.4.3	La solution doit permettre à l'utilisateur d'examiner le contenu qui a été versé par les partenaires du P3, de modifier ce contenu et de le rendre accessible dans la base de connaissances.
4.8 Intelligence artificielle et apprentissage machine L'apprentissage machine (AM) peut être utilisé dans le cadre de plusieurs processus au sein de la SNC. Dans le cadre du processus de triage des observations, on peut utiliser l'AM pour déterminer la cote relative de l'observation sur les plans de la résolvabilité, de la gravité et du degré de priorité. Les algorithmes de l'AM peuvent également être utilisés pour prendre des décisions quant au flux des travaux, notamment au moment de déterminer les prochaines étapes du traitement d'une observation ou d'une demande de service, après le triage. L'objectif sera d'automatiser certaines des activités susmentionnées de prise de décisions à l'aide de l'AM afin de mettre en œuvre des processus automatisés qui s'adaptent et qui apprennent continuellement.	
4.8.1 Créer et maintenir des modèles d'apprentissage machine	
4.8.1.1	La solution doit permettre le déploiement de modèles d'apprentissage machine dans le cadre du processus de triage des renseignements reçus par la SNC. Dans le cadre du triage, on peut utiliser le processus d'AM pour évaluer et établir le degré de gravité et de priorité et proposer la prochaine étape pour le traitement des observations et des demandes de service. À cette fin, le processus d'AM peut se fonder sur les résultats du processus de TLN et sur les données provenant du dépôt de la SNC en matière de cybercriminalité.
4.8.1.2	La solution doit permettre le déploiement de modèles d'apprentissage machine dans le cadre des processus de TLN afin que le système s'adapte à de nouveaux sujets et indicateurs et à de nouvelles données observables. La solution doit également utiliser l'apprentissage machine pour reconnaître les écarts dans les valeurs des éléments de données qui ont la même signification.
4.8.1.3	La solution doit aider la GRC à se conformer aux principes directeurs du gouvernement du Canada sur l'utilisation de l'IA ainsi qu'à la Directive sur la prise de décision automatisée[1]. La solution sera évaluée en fonction de l'Évaluation de l'incidence algorithmique (EIA)[2] du SCT.
4.8.1.4	La solution doit faire en sorte que les décisions prises à l'aide l'IA puissent être expliquées. L'utilisation de méthodes pouvant être expliquées est requise (par opposition à une approche de type « boîte noire »), au cas où les décisions seraient remises en question dans le cadre d'une instance judiciaire.

[1] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592

[2] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/evaluation-incidence-algorithmique.html

Tableau C-4 : SNC — Capacités des services fonctionnels

4.8.1.5	La solution doit permettre à des modèles d'apprentissage machine d'être appliqués pour des motifs comme les suivants, sans s'y limiter : a. l'identification des précurseurs — lorsque les événements, lorsqu'ils surviennent, peuvent indiquer qu'une activité présentant un intérêt suivra; b. l'établissement des profils des victimes — lorsque différentes données démographiques peuvent exiger une variation dans les niveaux de soutien et les interventions du côté des organismes d'application de la loi; c. l'établissement des profils des auteurs malveillants — dans le but d'identifier une personne qui peut présenter une menace; d. la détermination des outils habilitants et de l'infrastructure criminelle – y compris les fournisseurs de services, les marchés de logiciels et de services sur le Web invisible et les intermédiaires, entre autres; e. l'établissement des profils des entités (p. ex. appareils, services, emplacements et autres acteurs « non humains » en matière de cybercriminalité); f. la réalisation de simulations statistiques — y compris la vérification d'hypothèses et l'analyse de scénarios; g. la caractérisation d'événements comme la modification de la signature au fil du temps; h. la réalisation d'activités de renseignement – y compris l'élaboration de flux d'activités, de flux de marchandises, d'analyses des tendances criminelles, d'analyses financières et de profils de marché, entre autres; i. l'optimisation des recherches; j. la reconnaissance optique des caractères (ROC); k. l'automatisation de l'optimisation des intrants et de la réponse; l. la réalisation d'analyses des sentiments et d'analyses sémantiques; m. des fonctionnalités de traduction et d'accessibilité.
4.8.1.6	La solution doit permettre de rédiger facilement le code des modèles d'apprentissage machine ainsi que de former, de mettre à l'essai, d'optimiser (p. ex. l'optimisation des hyperparamètres) facilement ces modèles et de les déployer en production (p. ex. composante du triage et de la gestion des décisions) à partir de l'environnement de science des données (voir le point 4.3.1).
4.8.1.7	La solution doit permettre de sauvegarder, de créer des versions et de récupérer les modèles d'apprentissage machine à partir de l'environnement de science des données, ainsi que de faire le suivi des versions au moyen d'indicateurs et de mesures de rendement après le déploiement en production (p. ex. composante du triage et de la gestion des décisions).
4.9 Traitement du langage naturel (TLN) On utilisera le TLN pour mener des activités d'analyse de texte qui permettront d'extraire des données et des connaissances utiles à partir de texte non structuré. L'objectif du TLN est de réduire le fardeau des activités manuelles de parsage, d'analyse et de recherche de données tout en augmentant la capacité du GNCC de produire des renseignements à partir de sources volumineuses de données brutes. La fonction d'analyse de texte du GNCC sera automatisée, plus rapide et plus précise qu'une solution manuelle d'analyse de texte.	
4.9.1 Extraire les données et reconnaître les sujets	
4.9.1.1	La solution doit utiliser le TLN et l'analyse de texte afin de fournir des capacités d'extraction automatique de données d'entités nommées pour extraire des données relatives à la cybercriminalité, comme des données observables sur la cybercriminalité; des

Tableau C-4 : SNC — Capacités des services fonctionnels

	indicateurs; des incidents; des cibles; des tactiques, techniques et procédures (TTP) antagonistes et défensives; des campagnes; des plans d'action; et des auteurs malveillants, à partir de données non structurées (texte et images).
4.9.1.2	La solution doit utiliser le TLN pour fournir des capacités d'extraction automatique de données d'entités nommées afin d'extraire des données sur les observations et les demandes de service à partir de texte libre, aux fins du classement par type des demandes de service ou d'observations (p. ex., par type de crime).
4.9.1.3	La solution doit reconnaître le sentiment et envoyer des notifications en fonction des règles opérationnelles configurées par l'utilisateur (p. ex. reconnaissance de l'automutilation, de la violence, des menaces).
4.9.1.4	La solution doit offrir aux utilisateurs des outils permettant de surveiller, d'évaluer et de modifier au besoin les processus d'apprentissage machine.
4.9.1.5	La solution doit offrir une capacité de transcription automatisée.
4.9.1.6	La solution doit être en mesure d'identifier le texte ne provenant pas d'un locuteur natif dans un fichier texte.
4.9.1.7	La solution doit être en mesure d'identifier la ou les langues parlées dans un fichier audio.
4.9.1.8	La solution doit être en mesure d'identifier les différents locuteurs dans un fichier audio.
4.9.1.9	La solution doit automatiquement valider les données pour identifier les soumissions frivoles ou les valeurs frivoles dans les soumissions. Par exemple, elle doit cibler les signalements publics dont la perte est exagérée ou qui ne sont pas liés à la cybercriminalité ou à la fraude (par exemple, le vol de vélo). Ces règles de validation doivent être configurables. Remarque : Cela permettra de signaler plus précisément les pertes dues à la cybercriminalité et à la fraude.
4.10 Renseignement opérationnel Le système fournira de l'information pour soutenir le renseignement opérationnel (RO) au moyen de rapports, de tableaux de bord et d'autres outils. Le RO vise à fournir des indicateurs de rendement relatifs aux tendances opérationnelles ou en matière de cybercriminalité et de fraude au sein du GNCC, à l'échelle locale et nationale, ainsi que des indicateurs relatifs aux flux des travaux opérationnels — fonctions automatisées et manuelles, de l'information pour que les partenaires visés du GNCC prennent connaissance de la situation, un examen et l'élaboration de politiques stratégiques, et de l'analyse statistique en matière de cybercriminalité et de fraude (public canadien, communauté du renseignement).	
4.10.1 Fournir un accès aux rapports	
4.10.1.1	La solution doit être en mesure de produire et de diffuser en temps réel des rapports ponctuels et personnalisés.
4.10.1.2	La solution doit fournir des rapports, y compris les suivants, sans s'y limiter : a. un rapport sur les tendances et les statistiques en matière de cybercriminalité et de fraude pour répondre aux besoins opérationnels (p. ex. nombre de recherches au moyen du Portail des partenaires et des policiers, nombre de nouveaux logiciels malveillants identifiés) et stratégiques (p. ex. nombre annuel de renvois clos, en cours ou à l'égard desquels aucune mesure n'a été prise);

Tableau C-4 : SNC — Capacités des services fonctionnels

	b. un rapport fournissant des indicateurs quant aux observations, aux demandes d'aide, aux recherches effectuées, aux conflits éliminés, aux enquêtes en cours et terminées, aux partenariats établis et à la mobilisation des partenaires du secteur privé; c. des bulletins sur la cybercriminalité ou la fraude destinés à différents publics, y compris les utilisateurs du Portail des partenaires et des policiers, ou au grand public, par l'entremise du portail de sensibilisation du site Web de signalement public; d. l'enregistrement de statistiques et de métadonnées connexes fondées sur les données en matière de cybercriminalité et de fraude fournies par les partenaires et les intervenants en matière de cybercriminalité; e. des données sur la cybercriminalité et la fraude au Canada, lesquelles sont fournies au Centre canadien de la statistique juridique de Statistique Canada (il faudrait peut-être élaborer un format prescrit pour cet échange de données); f. la capacité de générer du contenu sous la forme de graphiques au sein des rapports, y compris, sans s'y limiter, des graphiques, des diagrammes, des tableaux et des produits d'extrants générés à partir des outils de visualisation (voir la capacité 4.3.4).
4.10.2 Sortir les résultats des rapports	
4.10.2.1	La solution doit permettre à l'utilisateur du GNCC d'examiner le contenu des rapports et des publications.
4.10.2.2	La solution doit permettre à l'utilisateur du GNCC de diffuser et transmettre les rapports au besoin.
4.10.3.3	La solution doit, en fonction des règles opérationnelles, transmettre automatiquement les rapports aux parties désignées (p. ex. les rapports à Statistique Canada).
4.10.3.4	La solution doit permettre à l'utilisateur de joindre des rapports aux fichiers.
4.10.3.5	La solution doit permettre à un utilisateur d'exporter des rapports dans divers formants (p. ex. Excel, CSV, PDF).
4.11 Recoupement des logiciels malveillants Permettre de faire une comparaison entre des échantillons de logiciels malveillants fournis par des organismes canadiens d'application de la loi et les données figurant dans les rapports sur les logiciels malveillants présentés par des services de police et figurant dans un dépôt national, ainsi que dans des solutions nationales et internationales choisies relatives aux logiciels malveillants.	
4.11.1 Examiner les demandes de recoupement des logiciels malveillants	
4.11.1.1	La solution doit permettre à l'utilisateur du GNCC de choisir une demande particulière dans une liste de demandes d'identification de logiciels malveillants.
4.11.1.2	La solution doit permettre à l'utilisateur du GNCC d'examiner la demande et de consigner toutes les notes ou observations requises.
4.11.1.3	La solution doit permettre à l'utilisateur du GNCC de cerner et de stocker les indicateurs de compromission qui n'ont pas été extraits automatiquement durant le processus de réception et de triage des observations.
4.11.1.4	La solution doit permettre à l'utilisateur du GNCC de modifier l'indice de gravité et de priorité de l'observation qui a été établi durant le processus de réception et de triage.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.11.1.5	La solution doit offrir une option permettant d'afficher des données traduites (en anglais ou en français) lorsqu'un utilisateur consulte un fichier contenant des langues étrangères.
4.11.2 Relever les correspondances avec les données de la SNC	
4.11.2.1	La solution doit mener automatiquement une recherche dans le dépôt de données pour relever les correspondances entre la valeur de hachage de l'échantillon de logiciel malveillant et d'autres indicateurs de compromission, ainsi que des données déjà stockées dans le dépôt de données.
4.11.2.2	La solution doit permettre à l'utilisateur du GNCC de mener d'autres recherches dans le dépôt de données au besoin.
4.11.2.3	La solution doit mettre à jour l'observation en y ajoutant les résultats des recherches automatisées et manuelles.
4.11.2.4	La solution doit permettre, dans les cas où aucune correspondance n'est relevée quant à la valeur de hachage soumise, à l'utilisateur du GNCC de créer une notification au moyen du P3, laquelle sera envoyée à l'organisme qui a présenté la demande et contiendra des directives sur la façon de soumettre l'échantillon de logiciel malveillant au GNCC.
4.11.2.5	La solution doit recevoir l'échantillon de logiciel malveillant dans une « boîte de dépôt » sécurisée. Remarque : le système doit isoler de façon sécuritaire les échantillons de logiciels malveillants de l'environnement organisationnel de TI de la GRC.
4.11.2.6	La solution doit générer une valeur de hachage pour le fichier reçu et la stocker dans le dépôt de données.
4.11.3 Utiliser un service d'analyse externe	
4.11.3.1	La solution doit permettre à l'utilisateur du GNCC d'envoyer une demande avec l'échantillon de logiciel malveillant soumis à un service externe d'analyse des logiciels malveillants, tout en faisant en sorte que l'échantillon demeure en isolement physique.
4.11.3.2	La solution doit stocker les résultats de l'analyse dans le dépôt de données une fois que les résultats de l'analyse ont été reçus.
4.11.3.3	La solution doit alerter l'utilisateur du GNCC si aucune réponse n'est reçue du service d'analyse des logiciels malveillants après un délai configurable.
4.11.4 Évaluer et renvoyer les résultats	
4.11.4.1	La solution doit permettre à l'utilisateur du GNCC d'examiner les résultats des recherches d'enrichissement et de l'analyse du logiciel malveillant (si un échantillon a été analysé).
4.11.4.2	La solution doit permettre à l'utilisateur du GNCC de créer un rapport d'analyse du logiciel malveillant, dont le contenu comprend la version du logiciel malveillant, un résumé, les conclusions et les recommandations.
4.11.4.3	La solution doit permettre à l'utilisateur du GNCC d'envoyer le rapport d'analyse du logiciel malveillant à l'organisme qui a présenté la demande.

Tableau C-4 : SNC — Capacités des services fonctionnels

4.11.5 Aviser les parties concernées	
4.11.5.1	La solution doit permettre à l'utilisateur du GNCC d'envoyer le rapport d'analyse du logiciel malveillant aux partenaires d'application de la loi.
4.11.5.2	La solution doit permettre à l'utilisateur du GNCC de créer un bulletin sur les logiciels malveillants et de publier ce bulletin sur le P3 en fonction des résultats de l'analyse.
4.12 Enrichissement automatisé Permet la résolution et l'enrichissement automatisés des données à l'aide de techniques fondées sur l'IA, y compris la résolution d'entités et l'analyse de réseaux.	
4.12.1 Résoudre les entités	
4.12.1.1	La solution doit être en mesure de résoudre automatiquement les entités (p. ex. éliminer les conflits quant à une identité en ligne, combiner un « John Smith » et un « J. Smith » qui vivent tous les deux à la même adresse).
4.12.1.2	La solution doit permettre à l'utilisateur d'examiner les entités résolues et de séparer les entités qui ont été regroupées à tort sous une entité unique.
4.12.1.3	La solution doit établir automatiquement les correspondances entre les données extraites et les données qui existent déjà dans le dépôt des cyberdonnées de la SNC et envoyer des notifications aux utilisateurs du GNCC à des fins d'examen (p. ex. à la suite d'un processus de TLN, d'une recherche de correspondances ou d'une analyse de données).
4.12.1.4	La solution doit permettre à l'utilisateur de voir et de manipuler les entités à l'aide d'un outil de visualisation des liens et réseaux.
4.12.1.5	La solution doit permettre d'identifier le service de police compétent à l'aide des attributs du fichier et des indicateurs de compromission, comme l'emplacement géographique, l'adresse municipale, l'adresse postale et l'adresse IP. P. ex. à l'aide de l'adresse des victimes dont il est question dans un fichier, identifier automatiquement tous les services de police compétents responsables du territoire où vivent les victimes, afin de faciliter la communication, le renvoi et la coordination.
4.12.2 Résoudre les réseaux	
4.12.2.1	La solution doit être en mesure d'identifier automatiquement les liens entre les entités résolues (p. ex. des renseignements d'identité semblables).
4.12.2.2	La solution doit permettre à l'utilisateur d'examiner les liens cernés et de séparer les entités qui ont été considérées à tort comme étant liées.
4.12.2.3	La solution doit permettre à l'utilisateur de voir et de manipuler les liens à l'aide d'un outil de visualisation des liens et réseaux.

C.6 SNC – Capacités techniques/de la solution

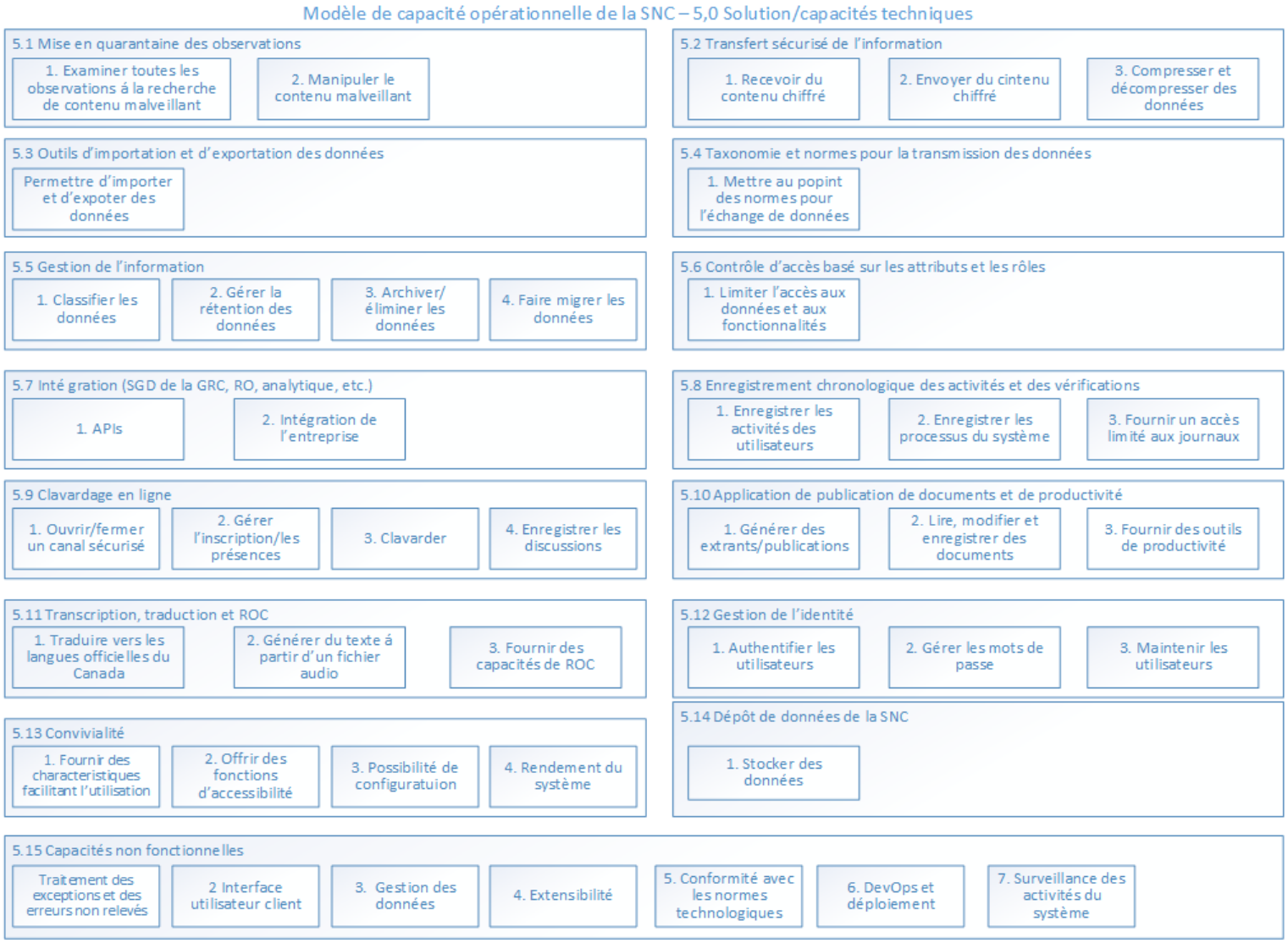


Figure C-6 : SNC – Capacités techniques/de la solution

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.1 Mise en quarantaine des observations La solution analysera toutes les observations (y compris les données importées à partir de supports physiques et de fichiers volumineux) à la recherche de contenu malveillant, de façon à cerner les observations potentiellement malveillantes et de permettre d'examiner ces observations avant de poursuivre le traitement.	
5.1.1 Examiner toutes les observations à la recherche de contenu malveillant	
5.1.1.1	La solution doit examiner automatiquement toutes les observations (y compris les pièces jointes) afin d'établir si elles comportent du contenu malveillant.
5.1.1.2	La solution doit stocker les résultats de l'analyse aux fins de l'examen des observations considérées comme malveillantes.
5.1.1.3	La solution doit intégrer automatiquement les observations non malveillantes aux fins de leur traitement.
5.1.1.4	La solution doit retenir aux fins d'un examen par l'utilisateur toute soumission qui comporte du contenu malveillant.
5.1.1.5	La solution doit analyser les observations à la recherche de contenu montrant une situation d'exploitation. Si un tel contenu est relevé, la solution doit transmettre l'observation au Centre national contre l'exploitation d'enfants (CNCEE) (le contenu pourrait être lié à l'exploitation de personnes vulnérables).
5.1.1.6	La solution doit permettre à l'utilisateur de transmettre du contenu montrant une situation d'exploitation au CNCEE, dans les cas où la solution n'a pas reconnu automatiquement le contenu montrant une situation d'exploitation.
5.1.2 Manipuler le contenu malveillant	
5.1.2.1	La solution doit permettre à l'utilisateur d'examiner les observations qui ont été identifiées comme comportant du contenu malveillant.
5.1.2.2	La solution doit permettre à l'utilisateur de retirer les pièces jointes malveillantes et d'intégrer l'observation modifiée.
5.2 Transfert sécurisé de l'information La solution doit être en mesure de transférer (recevoir ou envoyer) de façon sécuritaire de l'information avec les partenaires en utilisant Pretty Good Privacy (PGP) et la norme de chiffrement de source ouverte x.509.	
5.2.1 Recevoir du contenu chiffré	
5.2.1.1	La solution doit être en mesure de déchiffrer le contenu reçu aux fins du traitement par la SNC (p. ex., les courriels, les pièces jointes, les fichiers et les signatures numériques cryptés).
5.2.1.2	La solution doit garantir que les fichiers déchiffrés ne comportent pas de contenu malveillant.
5.2.1.3	La solution doit être compatible avec les normes de chiffrement de sources ouvertes de la GRC et PGP.
5.2.2 Envoyer du contenu chiffré	

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.2.2.1	La solution doit être en mesure de chiffrer le contenu envoyé généré par la SNC ou par un utilisateur du GNCC.
5.2.2.2	La solution doit être en mesure d'envoyer du contenu chiffré (p. ex. courriels chiffrés, pièces jointes, fichiers, signatures numériques cryptés)
5.2.2.3	La solution doit permettre l'utilisation de clés publiques à vérifier et à partager entre l'expéditeur et le destinataire. Doit être compatible avec X.509 et PGP.
5.2.2.4	La solution doit permettre l'entretien de clés publiques, y compris le stockage sur un serveur de cryptage à la GRC à des fins de récupération et d'identification.
5.2.2.5	La solution doit être intégrée à Microsoft Outlook afin de fournir une méthode de transmission d'informations sécurisée éliminant les informations en texte clair.
5.2.3 Compresser et décompresser des données	
5.2.3.1	La solution doit être en mesure de compresser des données en utilisant des normes comme les suivantes, sans s'y limiter : .ZIP, .LZH.
5.2.3.2	La solution doit être en mesure de décompresser des données en utilisant des normes comme les suivantes, sans s'y limiter : .ZIP, .LZH.
5.2.3.3	La solution doit permettre l'échange de textes d'agenda, de pièces jointes, de fichiers zippés et compressés cryptés (non envoyés en clair).
5.3 Outils d'importation et d'exportation des données La solution doit être en mesure d'intégrer et de transférer des données au moyen d'un support physique et de façon électronique (p. ex. sources ouvertes en ligne ou sources de données internes), ce qui comprend des transferts de fichiers volumineux (p. ex. au moins > 1 téraoctet).	
5.3.1 Permettre d'importer et d'exporter des données	
5.3.1.1	La solution doit être en mesure d'importer et d'exporter des données en provenance et à destination de la SNC (y compris les données existantes recueillies au moyen de la solution initiale de capacité opérationnelle).
5.3.1.2	La solution doit être en mesure d'exporter des données au moyen d'une capacité permettant d'extraire, de transformer et de charger, à même la solution ou au moyen d'autres plateformes commerciales (p. ex. DataStage d'IBM, produits de sources ouvertes).
5.3.1.3	La solution doit être en mesure de générer le fichier exporté sous un format commun (p. ex. XML, JSON) qui permet l'importation par un système externe (p. ex. SGC, outils d'analyse, MISP).
5.3.1.4	La solution doit être en mesure de charger les données de référence et les données opérationnelles reçues en masse (p. ex. plus de 1 téraoctet) d'organismes d'application de la loi, de partenaires, d'utilisateurs ou d'un dictionnaire de données en matière de cybercriminalité, par l'entremise d'une API et d'une interface de masse.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.3.1.5	La solution doit permettre l'importation de données à partir de supports physiques, de pièces jointes à un courriel, de fichiers transmis par l'entremise du P3, de flux de données de sources ouvertes, d'autres portails d'application de la loi (p. ex. SIENA, MISP) et de flux de données.
5.3.1.6	La solution doit permettre de gérer de façon sécuritaire toutes les données importées, y compris les échantillons de logiciels malveillants.
5.3.1.7	La solution doit permettre d'exporter les données sélectionnées de la SNC vers un outil d'analyse ou un dépôt désigné par la GRC aux fins d'analyse.
5.3.1.8	La solution doit permettre d'importer les résultats de l'analyse dans le dépôt de la SNC.
5.3.1.9	La solution doit permettre d'exporter des données choisies de la SNC vers un portail d'application de la loi choisi (p. ex. SIENA) ou une plateforme d'échange de données (p. ex. MISP).
5.3.1.10	La solution doit permettre de s'abonner à des sources d'information (p. ex. courriel ou groupe de contacts) afin d'importer du contenu de courriels ou de discussions.
5.4 Taxonomie et normes pour la transmission de données Le système doit être en mesure d'échanger des données en respectant les normes prescrites en matière d'échange de données.	
5.4.1 Mettre au point des normes pour l'échange de données	
5.4.1.1	La solution doit être en mesure d'échanger des données avec des organisations partenaires en utilisant la taxonomie (normes pour l'échange de données) élaborée par le GNCC et les partenaires nationaux et internationaux pour les données en matière de cybercriminalité.
5.4.1.2	La solution doit permettre à la GRC de définir et de maintenir les normes relatives à l'échange de données qui peuvent être utilisées pour importer et exporter des données à destination et en provenance du GNCC.
5.4.1.3	La solution doit être compatible avec les normes relatives à l'échange de données suivantes, sans s'y limiter : a. Structured Threat Information eXpression (STIX), b. Malware Information Sharing Platform (MISP); c. Vocabulary for Event Recording and Incident Sharing (VERIS); d. National Information Exchange Model (NIEM); e. Trusted Advance eXchange of Indicateurs Information (TAXII); f. Law Enforcement Information Data Standard (LEIDS).

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.5 Gestion de l'information Le système sera en mesure de gérer le cycle de vie de l'information du GNCC de la réception et création de l'information à son élimination. Le dépôt de données de la SNC soutiendra l'ensemble du cycle de vie des entités d'information intégrées ou créées à la suite du traitement d'observations ou de demandes de service en matière de cybercriminalité.	
5.5.1 Classifier les données	
5.5.1.1	La solution doit être en mesure d'utiliser des systèmes de catégorisation des données comme le Traffic Light Protocol, les désignations de sécurité des renseignements du gouvernement du Canada et les codes de traitement d'Europol (comme indiqué par l'émetteur des données) afin de régir l'échange de renseignements.
5.5.1.2	La solution doit confirmer que toutes les données reçues contiennent des codes relatifs au traitement des données et à la désignation de sécurité ou qu'elles sont étiquetées à cet égard.
5.5.1.3	La solution doit permettre à l'utilisateur d'étiqueter et de gérer les métadonnées des actifs de données du GNCC (p. ex. catalogage des données).
5.5.1.4	La solution doit permettre d'indiquer qu'un fichier contient un sujet (suspect ou victime) qui a moins de 18 ans (« l'âge d'une jeune personne »). L'âge d'une jeune personne doit être configurable.
5.5.1.5	La solution doit permettre d'attribuer plusieurs catégories à chaque élément d'information (p. ex. TLP = Rouge, code H3 d'Europol et cote Protégé B du gouvernement du Canada)
5.5.1.6	La solution doit permettre à l'utilisateur de modifier la catégorie des données, la catégorie au titre du TLP, la désignation de sécurité des renseignements du gouvernement du Canada ou le code de traitement d'Europol, au besoin.
5.5.2 Gérer la rétention des données	
5.5.2.1	La solution doit gérer la rétention des données en fonction de calendriers et de dates configurables en matière de rétention et d'élimination, lesquels sont établis par les émetteurs des données.
5.5.2.2	La solution doit protéger l'information et les données d'une perte accidentelle et de la corruption (p. ex. dialogues de confirmation dans l'interface utilisateur, intégrité référentielle).
5.5.2.3	La solution doit permettre à l'utilisateur d'éliminer manuellement des données en fonction de demandes approuvées d'élimination.
5.5.2.4	La solution doit permettre à l'utilisateur de désigner manuellement des renseignements comme étant retenues en fonction de demandes approuvées de retenue.
5.5.2.5	La solution doit être en mesure d'aviser automatiquement l'utilisateur autorisé du GNCC si des renseignements excèdent la désignation de sécurité Protégé B, en plus de permettre de réétiqueter, d'exporter et d'éliminer ces renseignements (p. ex. si un fichier est maintenant désigné Protégé C).
5.5.3 Archiver et éliminer les données	

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.5.3.1	La solution doit être en mesure d'archiver automatiquement des données dans l'unité de stockage des données à froid (« archives ») en fonction de délais configurables.
5.5.3.2	La solution doit être en mesure de fixer automatiquement une période de rétention des données en fonction de délais configurables.
5.5.3.3	La solution doit éliminer les renseignements et les données à la fin de leur période de rétention.
5.5.3.4	La solution doit cerner les renseignements et les données qui répondent aux critères pour l'archivage.
5.5.3.5	La solution doit être en mesure de fournir un processus de confirmation de l'élimination des données afin de permettre à l'utilisateur d'approuver l'élimination des données et de modifier la date d'aliénation des données, au besoin.
5.5.3.6	La solution doit tenir compte des liens au moment de cerner les données à éliminer. S'il existe un lien, les données liées sont assujetties à la date de rétention la plus éloignée.
5.5.3.7	La solution doit être en mesure de récupérer des données de l'unité de stockage des données froides pour les verser dans l'unité de stockage des données à chaud.
5.5.4 Faire migrer les données	
5.5.4.1	La solution doit être en mesure d'accéder aux données qui sont recueillies durant la période initiale de capacité opérationnelle.
5.5.4.2	La solution doit être en mesure d'accéder aux données qui sont recueillies par le Centre antifraude du Canada (CAFC) et le site Web de signalement public.
5.6 Contrôle d'accès basé sur les attributs et les rôles La solution utilisera le contrôle d'accès basé sur les rôles et le contrôle d'accès basé sur les attributs pour limiter l'accès aux fonctionnalités et aux données. Les règles relatives au RBAC et à l'ABAC peuvent être mises en œuvre pour restreindre l'accès en fonction d'attributs comme l'identificateur, le rôle ou le territoire de compétence de l'utilisateur.	
5.6.1 Limiter l'accès aux données et aux fonctionnalités	
5.6.1.1	La solution doit limiter l'accès des fonctionnalités aux utilisateurs en fonction des rôles assignés à ceux-ci.
5.6.1.2	La solution doit limiter l'accès de l'utilisateur aux renseignements, y compris les données, les fichiers et les projets, en fonction des rôles de l'utilisateur et en appliquant le contrôle d'accès basé sur les attributs (ABAC).
5.6.1.3	La solution doit comprendre des comptes d'utilisateur configurables et offrir la flexibilité requise pour permettre à différents niveaux d'utilisateurs d'accéder aux tableaux de bord.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.7 Intégration (SGD de la GRC, RO, analytique) La solution s'intégrera au système d'entreprise de la GRC et aux systèmes de certains partenaires (p. ex. SGD, Renseignements criminels, Renseignements sur la cybercriminalité, Gestion de cas), dont le système de téléphonie numérique du Centre d'appels, en utilisant des normes de sources ouvertes, s'il y a lieu.	
5.7.1 API	
5.7.1.1	La solution doit utiliser des interfaces de programmation d'application (API) qui respectent les normes du gouvernement du Canada sur les API aux fins de l'intégration dans le système des composantes, des outils utilisés par le GNCC et des plateformes externes.
5.7.1.2	La solution doit permettre l'échange de données avec des systèmes externes au moyen d'API et produire des rapports dans plusieurs domaines d'information, comme les systèmes de gestion des dossiers de la police, ainsi que d'autres ministères ou d'autres partenaires en matière de cybercriminalité (p. ex. entreprises de cybersécurité, institutions financières).
5.7.1.3	La solution doit s'intégrer au système organisationnel de courriel de la GRC afin d'intégrer les observations et les demandes de service, ainsi que de permettre aux utilisateurs de communiquer avec les partenaires en matière de cybercriminalité.
5.7.1.4	La solution doit permettre de créer des API externes et synchrones de service Web au moyen de normes ouvertes de l'industrie lorsque la source autorisée des données et des fonctionnalités se trouve dans d'autres systèmes.
5.7.1.5	La solution doit, pour toutes les API, donner accès à des données sous la forme d'entités opérationnelles ou de schémas d'objet non exclusifs. Plus précisément, les API doivent pouvoir résumer les tableaux et les structures de données brutes principaux.
5.7.2 Intégration de l'entreprise	
5.7.2.1	La solution doit être en mesure d'utiliser un gestionnaire d'événements pour gérer toutes les interactions entre les composantes au sein de la solution, à l'aide de messages d'événements asynchrones.
5.7.2.2	La solution doit être en mesure d'utiliser une connexion spécialisée au nuage pour faire en sorte qu'une connexion sécurisée haute vitesse existe entre le centre de données de la GRC et l'espace infonuagique Protégé B de la GRC.
5.7.2.3	La solution doit s'intégrer avec des outils de gestion et de gouvernance des données d'entreprise de tierces parties.
5.7.2.4	La solution doit s'intégrer à des services géospatiaux de tierces parties.
5.7.2.5	La solution doit permettre l'accès à toutes les API au moyen de liaisons et de protocoles standards ouverts (y compris, sans s'y limiter, le transfert d'état représentationnel [REST]/la notation des objets du langage Java [JSON] et le langage de balisage extensible [XML]).
5.7.2.6	La solution doit être compatible avec le chiffrement au titre du protocole de sécurité de la couche transport (TLS) 1,2 pour l'ensemble des interfaces, en tant que niveau minimal de sécurité de la connexion.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.8 Enregistrement chronologique des activités et des vérifications La solution doit enregistrer toutes les activités des utilisateurs et du système dans des journaux d'activités. L'activité du système doit être enregistrée dans des journaux de vérification du système.	
5.8.1 Enregistrer les activités des utilisateurs	
5.8.1.1	La solution doit enregistrer dans un journal toutes les activités effectuées par les utilisateurs du P3 et du GNCC, y compris les ajouts, les modifications, les recherches, les impressions, les exportations et la suppression de renseignements.
5.8.1.2	La solution doit permettre à l'utilisateur du GNCC de créer manuellement une activité qui ne serait autrement pas enregistrée dans le journal des activités du système (p. ex. appel téléphonique lié au fichier, recherche dans le système d'exploitation).
5.8.1.3	La solution doit faire en sorte que les fichiers des journaux d'activités sont immuables.
5.8.1.4	La solution doit faire en sorte que les journaux contiennent l'identificateur de l'utilisateur, la date et l'heure de l'activité et la tâche accomplie.
5.8.1.5	La solution doit enregistrer les paramètres des recherches effectuées dans le dépôt sur la cybercriminalité de la SNC.
5.8.1.6	La solution doit conserver toutes les versions d'un fichier si celui-ci est manipulé durant des activités d'extraction de renseignements.
5.8.1.7	La solution doit enregistrer tous les critères de recherche et tous les ensembles de résultats subséquents.
5.8.2 Enregistrer les processus du système	
5.8.2.1	La solution doit conserver un journal de toutes les activités effectuées automatiquement par le système.
5.8.2.2	La solution doit conserver un journal de vérification de toutes les activités effectuées dans toutes les bases de données de la solution.
5.8.2.3	La solution doit conserver un journal de vérification pour tous les accès au système par un utilisateur (p. ex. qui s'est connecté, l'heure de la connexion, l'heure de la déconnexion, les tentatives de connexion).
5.8.2.4	La solution doit faire en sorte que les fichiers des journaux de vérification sont immuables et accessibles en lecture seule.
5.8.2.5	La solution doit être en mesure d'envoyer des notifications aux utilisateurs administrateurs en cas de défaillance d'une composante du système ou de tentatives répétées d'un utilisateur qui donnent lieu à des messages d'erreur.
5.8.2.6	La solution doit fournir des interfaces qui permettent de gérer les situations de façon efficace lorsque des systèmes externes connaissent des défaillances ou ne sont pas disponibles.
5.8.3 Fournir un accès limité aux journaux	
5.8.3.1	La solution doit permettre à l'utilisateur autorisé du GNCC de voir le contenu des fichiers des journaux d'activités des utilisateurs.
5.8.3.2	La solution doit permettre à l'utilisateur autorisé (p. ex. les administrateurs de système) de voir le contenu des fichiers des journaux de vérification du système.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.9 Clavardage en ligne Le système fournira une fonctionnalité de clavardage sécurisé en temps réel pour les utilisateurs du GNCC et du P3. Cela comprend les utilisateurs du GNCC qui ne se trouvent pas au bureau principal du GNCC (p. ex. J-CAT).	
5.9.1 Ouvrir et fermer un canal sécurisé	
5.9.1.1	La solution doit permettre à l'utilisateur d'ouvrir et de fermer un canal sécurisé pour démarrer une séance de clavardage et y mettre fin.
5.9.1.2	La solution doit permettre à l'administrateur de la séance de clavardage d'inviter d'autres utilisateurs du GNCC à se joindre à la séance.
5.9.2 Gérer l'inscription et les présences	
5.9.2.1	La solution doit aviser les utilisateurs de la création d'une séance de clavardage à laquelle ils sont invités. L'utilisateur doit pouvoir accepter ou refuser l'invitation.
5.9.2.2	La solution doit permettre à l'utilisateur de se joindre à une séance de clavardage à laquelle il est invité ou de quitter une telle séance.
5.9.2.3	La solution doit permettre à l'administrateur de la séance de clavardage de voir une liste des utilisateurs qui participent actuellement à la séance de clavardage.
5.9.3 Clavardage	
5.9.3.1	La solution doit permettre l'échange sécurisé de messages texte (clavardage en groupe), ainsi que la tenue de téléconférences et de vidéoconférences.
5.9.3.2	La solution doit permettre l'intégration de liens aux messages envoyés durant une séance de clavardage (p. ex. liens vers des fichiers ou des projets).
5.9.4 Enregistrer des discussions	
5.9.4.1	La solution doit créer un registre immuable de tout le contenu généré par les participants à une séance de clavardage.
5.10 Applications de publication de documents et de productivité Pour mener ses activités, l'organisation devra avoir la capacité d'extraire le contenu des billets, des fichiers et des projets pour créer des copies électroniques et papier. Les activités exigent également l'utilisation d'un logiciel de « bureautique », comme un logiciel de traitement de texte ou un tableur électronique, permettant d'examiner les pièces jointes ou de modifier le contenu pour la production d'extrants. Le système doit permettre à l'utilisateur d'ouvrir facilement de telles pièces jointes ou de transférer des renseignements entre les pièces jointes et le système.	
5.10.1 Générer des extrants et des publications	
5.10.1.1	La solution doit permettre à l'utilisateur de modifier et de formater des documents à publier au moyen d'outils de traitement de texte.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.10.1.2	La solution doit être en mesure d'assembler les composantes d'un produit ou d'un courriel (y compris un courriel sécurisé) aux fins d'examen par l'utilisateur.
5.10.1.3	La solution doit être en mesure de créer des fichiers PDF de format standard (p. ex. demandes ou ordonnances de préservation des données), de les joindre à des courriels et de placer le courriel dans une file d'attente aux fins d'examen et d'envoi par l'utilisateur.
5.10.1.4	La solution doit être en mesure de produire les formulaires connexes de demande et d'ordonnance de préservation des données 5 001, 5 002, 5 003 et 5 009.
5.10.1.5	La solution doit permettre à l'utilisateur de créer un courriel (y compris un courriel sécurisé) et de l'envoyer à un partenaire en matière de cybercriminalité.
5.10.1.6	La solution doit automatiquement étiqueter les documents en fonction de la catégorie de sécurité des données (p. ex. niveaux de sécurité du gouvernement du Canada [Protégé A, B, C, Confidentiel, Secret et Très secret], les codes de traitement d'Europol [H1, H2 et H3] et le Traffic Light Protocol [Blanc, Vert, Orange et Rouge]) et laisser l'utilisateur passer outre à cette catégorie, au besoin.
5.10.2 Lire, modifier et enregistrer des documents	
5.10.2.1	La solution doit permettre à l'utilisateur d'ouvrir et de visualiser une pièce jointe au moyen du lecteur approprié.
5.10.2.2	La solution doit permettre d'« enregistrer sous », de sorte qu'un fichier puisse être converti vers un autre format (p. ex. un document Word converti en PDF).
5.10.2.3	La solution doit comprendre une fonctionnalité de vérification de l'orthographe, au moins en anglais et en français canadiens.
5.10.3 Utiliser des outils de productivité	
5.10.3.1	La solution doit permettre à l'utilisateur d'utiliser des outils pour calculer la valeur monétaire d'une transaction à la date où celle-ci a été entrée dans le système, en convertissant toute devise en dollars canadiens ou américains.
5.10.3.2	La solution doit fournir un environnement sécurisé de collaboration en temps réel qui permet, en temps réel et en simultané, l'accès aux outils, projets et artefacts par l'utilisateur autorisé du GNCC ou du P3, ainsi que leur modification et leur examen, la formulation de commentaires et la tenue de discussions à leur sujet. Les artefacts peuvent comprendre, sans s'y limiter, les documents texte, les feuilles de calcul, les fichiers PDF, les présentations ou les cartes de visualisation.
5.10.3.3	La solution doit être en mesure de maintenir l'historique et l'intégrité des modifications précédentes, au moyen de sa capacité de collaboration.
5.10.3.4	La solution doit permettre, au moyen de sa capacité de collaboration, à l'utilisateur d'afficher des outils et des artefacts et d'en faire la démonstration grâce à une fonctionnalité de partage d'écran.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.11 Transcription, traduction et ROC Pour mener ses activités, l'organisation doit pouvoir convertir des fichiers audio en texte, traduire des fichiers de texte vers l'anglais et le français et convertir des images contenant du texte imprimé ou manuscrit en données pouvant être utilisées par une machine.	
5.11.1 Traduire vers les langues officielles du Canada	
5.11.1.1	La solution doit être en mesure de traduire du texte de l'anglais au français et vice versa, conformément aux normes du gouvernement du Canada.
5.11.1.2	La solution doit être en mesure de traduire du texte en d'autres langues vers l'anglais ou le français. La liste des langues requises n'a pas encore été établie (p. ex. russe, espagnol, cantonais/mandarin, coréen, hindi, persan, allemand).
5.11.1.3	La solution doit stocker le texte traduit dans le fichier connexe de la SNC.
5.11.1.4	La solution doit conserver le texte original dans la langue initiale.
5.11.2 Générer du texte à partir d'un fichier audio	
5.11.2.1	La solution doit être en mesure de générer du texte à partir du fichier audio.
5.11.2.2	La solution doit stocker le texte généré dans le fichier connexe de la SNC.
5.11.2.3	La solution doit conserver le fichier audio original dans le fichier connexe de la SNC.
5.11.3 Fournir des capacités de ROC	
5.11.3.1	La solution doit permettre de convertir des images contenant du texte imprimé ou manuscrit en données pouvant être utilisées par une machine.
5.11.3.2	La solution doit permettre de balayer et de lire des codes QR afin de pouvoir utiliser les données qui s'y rattachent (p. ex. codes QR sur les « billets » Bitcoin ou des cartes-cadeaux).
5.12 Gestion de l'identité La création, la gestion et le maintien des identificateurs des utilisateurs (nom d'utilisateur et mot de passe) sont requis pour permettre la gestion de l'accès à la solution. Ces exigences sont fortement réglementées par l'environnement de la GRC et la Sous-direction de la sécurité ministérielle.	
5.12.1 Authentifier les utilisateurs	
5.12.1.1	La solution doit fournir une fonctionnalité de connexion (authentification), conformément aux normes et aux technologies approuvées par la GRC en matière de gestion de l'identité, y compris pour le P3.
5.12.1.2	La solution doit vérifier l'identité de l'utilisateur au moment de la connexion afin d'appliquer subséquemment les exigences relatives au RBAC dans la solution.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.12.2 Gérer les mots de passe	
5.12.2.1	La solution doit permettre à l'utilisateur de gérer ses mots de passe. La gestion des mots de passe doit être conforme aux normes de la GRC (p. ex. format, réinitialisation périodique).
5.12.2.2	La solution doit utiliser Azure Active Directory.
5.12.3 Maintenir les utilisateurs	
5.12.3.1	La solution doit permettre à l'utilisateur autorisé de voir, de créer, de suspendre ou de réintégrer un utilisateur du système de la SNC ou du P3, ou encore de modifier son profil.
5.12.3.2	La solution doit permettre à l'utilisateur autorisé de la GRC d'attribuer ou de retirer à un utilisateur une autorisation d'accès établie.
5.12.3.3	La solution doit permettre à un utilisateur autorisé de la GRC de vérifier l'identité des nouveaux utilisateurs et de gérer leurs clés publiques et privées (PGP et x.509), qu'elles soient attribuées ou fournies par l'utilisateur.
5.13 Convivialité Inclure des capacités liées à la facilité d'utilisation, à l'accessibilité, à l'aide en ligne, à une aide de deuxième niveau et au rendement.	
5.13.1 Fournir des caractéristiques facilitant l'utilisation	
5.13.1.1	La solution doit respecter les normes applicables du gouvernement du Canada quant à la convivialité des systèmes de TI en ce qui concerne l'accessibilité ainsi que l'apparence et le type d'environnement habituels. Ces normes sont inspirées des Règles pour l'accessibilité des contenus Web (WCAG) 2,0. La solution doit être conforme aux normes d'accessibilité du Web telles que décrites dans la norme du SCT sur l'accessibilité du Web[3].
5.13.1.2	La solution doit fournir à l'utilisateur une interface utilisateur personnalisable (p. ex. disposition des fenêtres, tableaux de bord, listes des travaux en attente, langue par défaut).
5.13.1.3	La solution doit fournir des interfaces utilisateurs comprenant des séquences utiles, des liens entre les renseignements, des centres d'intérêt, des messages et des avertissements aux utilisateurs, en plus d'offrir une apparence, un environnement, une navigation et une orientation uniformes et des écrans portant un titre.
5.13.1.4	La solution doit permettre à l'utilisateur d'accéder à une fonctionnalité d'aide en ligne qui tient compte du contexte.
5.13.1.5	La solution doit utiliser des listes déroulantes et des contrôles qui se remplissent automatiquement relativement aux données interrogeables et des widgets de gestion des données pour faciliter et normaliser la saisie de données.
5.13.1.6	La solution doit utiliser au maximum les données disponibles (comme les données des partenaires) afin de réduire au minimum l'entrée de données par les utilisateurs et d'optimiser l'exactitude.

[3] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.13.1.7	La solution doit permettre à l'utilisateur de créer un billet pour recevoir de l'aide des ressources d'appui du système de la SNC. Les billets d'aide peuvent être transmis au centre d'assistance central aux fins de traitement.
5.13.2 Offrir des fonctions d'accessibilité	
5.13.2.1	La solution doit fournir toutes les interfaces utilisateurs, tous les documents et toutes les ressources d'aide dans les deux langues officielles du Canada (anglais et français). Cela signifie que les utilisateurs qui choisissent le français comme langue d'affichage ne verront rien en anglais dans l'interface utilisateur graphique de la solution, ce qui comprend, sans s'y limiter, les fichiers d'aide, les tutoriels, les messages d'erreur et les renseignements juridiques (le contenu généré par les utilisateurs est exclu).
5.13.2.2	La solution doit être offerte et accessible aux personnes ayant des incapacités, conformément aux normes d'accessibilité 2.0 A.
5.13.2.3	La solution doit être offerte aux utilisateurs dans l'ensemble du Canada et à l'international.
5.13.3 Possibilité de configuration	
5.13.3.1	La solution doit permettre à l'utilisateur autorisé de maintenir des paramètres configurables (p. ex. listes de sélection de données, règles opérationnelles, modèles).
5.13.3.2	La solution doit, dans la mesure du possible, permettre de configurer le système sans entraîner d'arrêt du système ni de nouvelles versions du logiciel.
5.13.4 Rendement du système	
5.13.4.1	La solution doit permettre à au moins 500 utilisateurs d'utiliser la SNC et le P3 en même temps sans baisse de rendement.
5.13.4.2	La solution doit être en mesure de gérer l'utilisation simultanée des données lorsque plus d'un utilisateur accède au même fichier/aux mêmes données en même temps.
5.14 Dépôt de données de la SNC Le dépôt de données de la SNC contiendra l'ensemble des données opérationnelles du GNCC, y compris toutes les observations et demandes de service reçues, les métadonnées connexes et les artefacts numériques et produits opérationnels qui en découlent.	
5.14.1 Stocker des données	
5.14.1.1	La solution doit fournir un dépôt de données qui est en mesure de stocker de façon sécuritaire toutes les observations, demandes de service, pièces jointes et métadonnées, toutes les tâches et tous les résultats liés aux travaux et aux analyses, tous les journaux d'activités et de vérification et tous les produits du travail effectué par le système de la SNC et les utilisateurs de GNCC.
5.14.1.2	La solution doit stocker les données d'une façon sécuritaire, conformément aux normes du SCT.
5.14.1.3	La solution doit être en mesure de stocker les données qui sont reçues dans plusieurs langues, en conservant le jeu de caractères utilisé dans l'observation (p. ex. en plus du français et de l'anglais, permettre de stocker du contenu en russe, en espagnol, en cantonais/mandarin, en coréen, en hindi, en persan, en allemand).

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.14.1.4	La solution doit faire en sorte que toutes les données traitées, stockées, maintenues, dérivées et utilisées par la solution, y compris toutes les données stockées en ligne, données archivées et données de sauvegarde, demeurent au Canada.
5.14.1.5	La solution doit être en mesure de traiter les données dans des formats structurés et non structurés.
5.14.1.6	La solution doit être évolutive et élastique pour pouvoir gérer les fluctuations potentielles du volume des opérations et des données liées à la cybercriminalité.
5.14.1.7	La solution doit protéger les renseignements et les données contre des mesures et un accès non autorisés.
5.14.1.8	La solution doit protéger les renseignements et les données contre la perte accidentelle et la corruption.
5.15 Capacités non fonctionnelles Les capacités ci-dessous incluent les exigences non fonctionnelles relatives à l'interface utilisateur, à la gestion des données, à la conformité avec les normes du GC et à la surveillance du système.	
5.15.1 Traitement des exceptions et des erreurs non relevées	
5.15.1.1	La solution doit enregistrer toutes les exceptions non relevées relatives au temps d'exécution et tous les messages non relevés relatifs à la file d'attente des messages non distribués générés durant le traitement des transactions opérationnelles de la SNC.
5.15.1.2	Pour soutenir l'analyse des erreurs, la solution doit inclure des ID de corrélation dans ses messages afin de faciliter le suivi et l'enregistrement des événements au moyen du système.
5.15.1.3	La solution doit comprendre une fonction sécurisée de recherche des utilisateurs afin que les administrateurs de système puissent examiner la liste des erreurs et la mettre à jour une fois que les erreurs sont résolues.
5.15.2 Interface utilisateur client	
5.15.2.1	La solution doit fournir un client fondé sur un navigateur comme interface utilisateur, lequel doit être compatible, au minimum, avec : Microsoft Internet Explorer 11 pour Windows 64 bits et plus, Microsoft Edge, Firefox et Google Chrome 75 pour Windows 64 bits et plus.
5.15.2.2	La solution doit offrir un processus unique de connexion qui permet aux utilisateurs du GNCC et du P3 d'accéder à l'ensemble des fonctionnalités auxquelles ils ont accès au titre du RBAC sans se connecter plusieurs fois.
5.15.2.3	L'application client doit s'arrêter automatiquement après un délai d'inactivité configurable, après quoi l'utilisateur doit s'identifier de nouveau.
5.15.2.4	La solution doit protéger l'information par des méthodes sécurisées d'authentification, au moyen de normes ouvertes (y compris, sans s'y limiter, OpenID, OAuth ou SAML).
5.15.2.5	La solution doit fournir une notification d'occupation (p. ex. un sablier) lorsque le logiciel est occupé à effectuer une opération et que l'utilisateur doit attendre.

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.15.3 Gestion des données	
5.15.3.1	La solution doit étiqueter automatiquement les données lorsqu'elles sont intégrées dans la SNC afin de conserver la provenance des données (p. ex. horodateur, source du fournisseur des données et autres métadonnées utiles à des fins de vérification ou de surveillance).
5.15.3.2	La solution doit enregistrer et conserver les métadonnées sur la traçabilité et la provenance des données tout au long des processus de transformation et d'intégration des données, conformément à la Norme sur les métadonnées du gouvernement du Canada.
5.15.3.3	La solution doit comprendre des fonctions de validation des données et de surveillance de la qualité des données pour les processus d'enregistrement de données par lots et l'enregistrement de données en temps réel et quasi réel.
5.15.3.4	La solution doit fournir des interfaces pour la validation des opérations de nettoyage des données au moyen d'une source d'information normalisée (p. ex. adresses postales, géocodage, données démographiques, normes de la GRC sur les données).
5.15.3.5	La solution doit permettre la fédération de données en fournissant un accès virtuel à des structures de bases de données, y compris des données semi-structurées, et avoir la capacité de lier des données pour un accès et une analyse en temps réel.
5.15.3.6	La solution doit permettre l'optimisation des recherches, tant automatiquement dans le cadre de demandes provenant des SGBD que manuellement grâce à l'optimisation interne avancée des recherches créées manuellement.
5.15.4 Extensibilité	
5.15.4.1	La solution doit fournir à l'utilisateur administrateur la capacité de personnaliser les fonctionnalités de l'interface utilisateur (p. ex. ajouter des entités, des attributs et des entités logiques), à l'aide d'une approche exigeant peu de code ou n'exigeant aucun code.
5.15.5 Conformité avec les normes technologiques	
5.15.5.1	La solution doit respecter les Normes du gouvernement du Canada sur les API[4].
5.15.5.2	La solution doit respecter les normes et les lignes directrices du gouvernement du Canada quant au RBAC/ABAC. Consulter le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3)[5].
5.15.6 DevOps et déploiement	
5.15.6.1	Les applications de la solution doivent être regroupées dans des conteneurs d'un ou de plusieurs microservices avec des scripts paramétriques qui peuvent être adaptés à chaque environnement cible (p. ex. contrôle de la qualité [CQ], production).
5.15.6.2	Chaque version doit comprendre des documents fournissant l'ensemble des scripts et des changements.

[4] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html

[5] https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de

Tableau C-5 : MCO de la SNC – Capacités techniques/de la solution

5.15.6.3	Les scripts d'installation et de version doivent être présentés dans un format de code lisible et déployés en tant que trousse pour mettre en place la solution dans l'environnement approprié.
5.15.6.4	Les scripts relatifs aux mises à jour et correctifs doivent être présentés dans un format de code lisible et sous la forme d'une trousse pour être déployés dans le cadre de la mise à jour de l'application.
5.15.6.5	Chaque composante qui doit être installée sur un serveur différent doit avoir son propre script de version, présenté sous un format de code lisible.
5.15.6.6	Chaque version doit respecter les exigences relatives au dépôt de code de la GRC et la méthodologie de lancement des versions de l'organisation.
5.15.7 Surveillance des activités du système	
5.15.7.1	La solution doit permettre de surveiller les connexions, la taille des bases de données, l'accès aux bases de données, l'usage de l'unité centrale et des ressources infonuagiques et le trafic sur le réseau.
5.15.7.2	La solution doit enregistrer les événements liés au système et à la sécurité.
5.15.7.3	La solution doit stocker tous les journaux d'activités et de système dans l'enregistreur chronologique de l'espace infonuagique Protégé B de la GRC.

APPENDICE D – DIAGRAMME DE L'ARCHITECTURE CONCEPTUELLE GÉNÉRALE

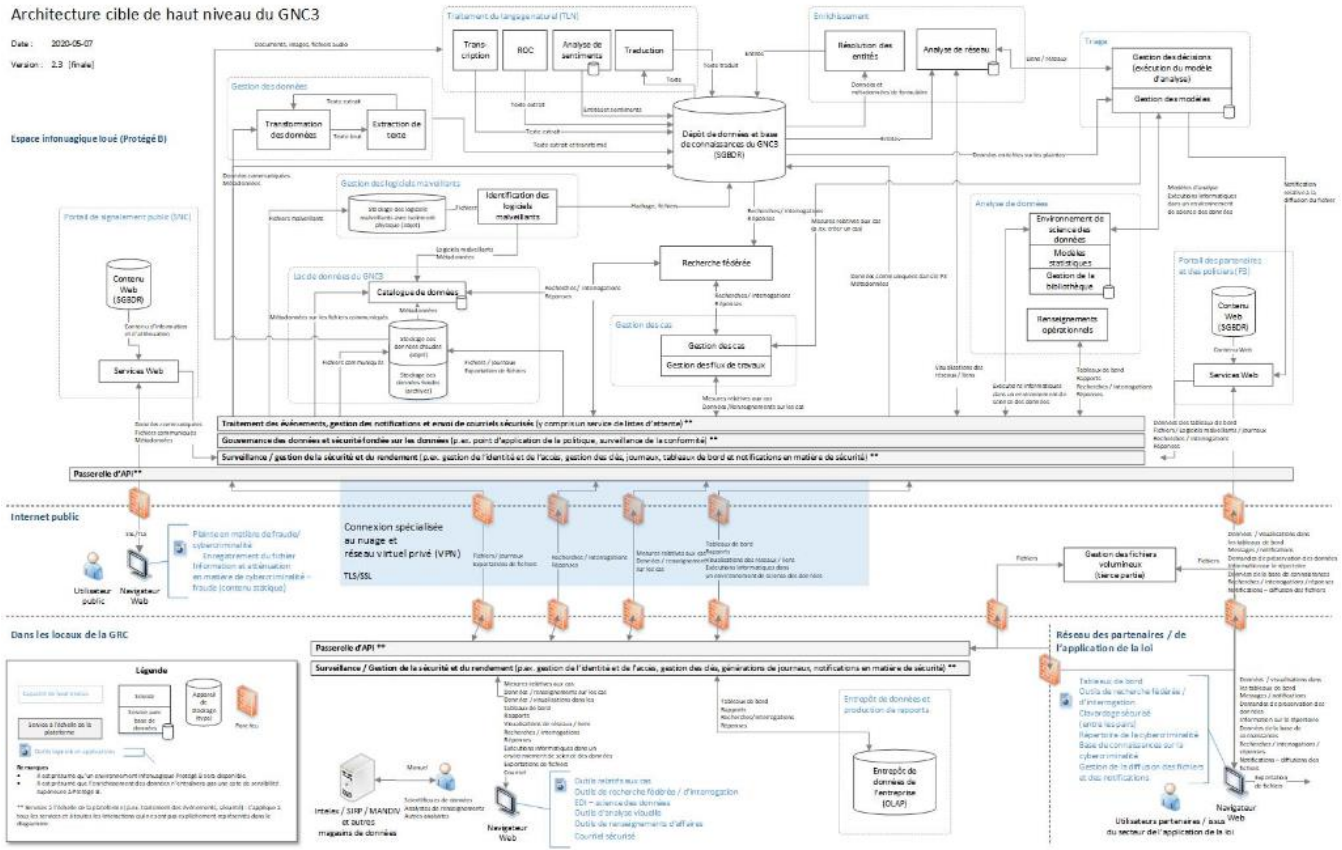


Figure D-1 : Architecture conceptuelle générale de la SNC

D.1 Description des composantes de l'architecture cible

a) Plusieurs des composantes universelles de la solution sont décrites selon une représentation générale afin d'augmenter la lisibilité et de réduire la complexité du diagramme, plus précisément :

   i) la passerelle d'API;

   ii) la surveillance et la gestion de la sécurité et du rendement;

   iii) la gouvernance des données et la sécurité axée sur les données;

   iv) le gestionnaire d'événements, la gestion des notifications et les courriels sécurisés.

b) On s'attend à ce que ces composantes universelles s'intègrent et interagissent avec presque l'ensemble des composantes de la solution; par conséquent, on les décrit comme une pile. On considère également qu'il s'agit des aspects les plus complexes de la solution, et il revient à l'entrepreneur de décider de la meilleure façon d'offrir cette fonctionnalité tout en respectant les exigences.

c) Une description de chaque composante de l'architecture cible est incluse dans le Tableau D 1 : Description des composantes de l'architecture, à des fins de référence.

Tableau D-1 : Description des composantes de l'architecture

Composante architecturale	Description
Portail de signalement public – Services Web	Cette composante sera élaborée à l'extérieur de la solution de l'entrepreneur et est incluse dans le diagramme parce qu'elle interagira avec la solution. Voir la Section 4.4 – Site Web de signalement destiné au public pour obtenir plus de renseignements. Cette composante élaborée par la GRC fournit un accès par navigateur et une application mobile permettant d'obtenir des renseignements sur les plaintes en matière de cybercriminalité et de fraude provenant de personnes et de petites ou moyennes entreprises (PME). Il s'agit d'un portail central et destiné au public pour la collecte de plaintes en matière de cybercriminalité et de fraude provenant de personnes et de PME à l'échelle du Canada.
P3 – Contenu Web	Cette composante fournit un accès à des répertoires liés à la cybercriminalité, à la base de connaissances du GNCC et à un catalogue des outils et services du GNCC.
P3 – Services Web	Cette composante fournit une voie de communication sécurisée et bilatérale entre la GRC et les partenaires de confiance en matière de cybercriminalité. Le P3 facilite la saisie de demandes de service et d'observations en matière de cybercriminalité ainsi que l'envoi de tels documents par des partenaires de confiance à la SNC. En outre, l'envoi de notifications aux partenaires de confiance en matière de cybercriminalité sera une capacité clé du P3. Les utilisateurs potentiels du P3 comprennent les organismes canadiens d'application de la loi, d'autres ministères (p. ex. le Centre canadien pour la cybersécurité [CCCS], le Conseil de la radiodiffusion et des télécommunications canadiennes [CRTC] et Statistique Canada) et les agents de liaison de la GRC en matière de cybercriminalité.

Tableau D-1 : Description des composantes de l'architecture

Composante architecturale	Description
Gestion des décisions	Cette composante fournit un mécanisme automatisé qui permet de générer des décisions en fonction de conditions (p. ex. des modèles et des règles). Elle permet de définir et d'exécuter des règles logiques, d'exécuter des modèles d'analyse en parallèle et de tenir un vote selon la méthode ensembliste afin de soutenir le processus décisionnel.
Gestion des modèles et exécution informatique	Cette composante gère et exécute des modèles d'analyse pour soutenir différentes fonctions de la composante de gestion des décisions. Elle déploie et retire des modèles, offre une fonction de création de versions et fait le suivi du rendement (p. ex. efficacité et erreurs) des modèles en production tout au long de leur cycle de vie.
Résolution des entités	Cette composante fournit une fonction automatisée de désambiguïsation, de regroupement, d'identification et de gestion des entités réelles (p. ex. des gens, des endroits et des choses) en liant ou en regroupant des éléments de données semblables en fonction d'un ensemble de règles prédéfinies.
Analyse de réseaux	Cette composante identifie les liens et les réseaux entre les entités réelles résolues (p. ex. des gens, des endroits et des choses) et en fait le suivi. Elle fournit un mécanisme permettant de déterminer le risque associé à une entité particulière en fonction d'associations avec d'autres entités du même réseau. Ces liens et réseaux sont affichés à l'aide d'un outil séparé pour la représentation graphique et l'affichage des réseaux et des liens entre les entités.
Transformation des données	Cette composante fournit des services de conversion, de nettoyage et d'intégration des données afin de transformer les données en les faisant passer d'un format à un autre et de les préparer pour le stockage et l'utilisation. Elle fournit également les mécanismes permettant d'intégrer des données provenant de différentes sources (p. ex. flux de données, supports physiques et fichiers volumineux).
Extraction de texte	Cette composante extrait du texte et des données de différentes sources (p. ex. documents, tableaux et champs de formulaires), de sorte que l'information soit facilement accessible aux fins d'utilisation.
Analyse des sentiments	Cette composante utilise un processus informatique pour cerner, catégoriser et noter les opinions exprimées dans le passage d'un texte afin de déterminer l'attitude de l'auteur à l'égard d'un sujet particulier (positive, négative, neutre).
Gestion des cas	Cette composante fournit des capacités de gestion centrales à l'égard des cas. Les cas sont des fichiers qui regroupent des données reliées sur un sujet d'intérêt (p. ex. un client), y compris, mais sans s'y limiter, des notes, des communications, des historiques, des coordonnées, des analyses et des conclusions. Cette composante fait également le suivi du statut de chaque cas (p. ex. nouveau, attribué et fermé) et gère ce statut, en plus d'aider l'utilisateur à prendre différentes mesures à l'égard d'un cas (p. ex. attribution, augmentation du niveau de priorité), parallèlement à la composante de gestion des flux des travaux.

Tableau D-1 : Description des composantes de l'architecture

Composante architecturale	Description
Gestion des flux des travaux	Cette composante fournit le mécanisme pour gérer les tâches ainsi que les entités logiques afin de diriger le flux entre les tâches. Elle peut être utilisée pour coordonner les billets liés à des observations et à des fichiers de renseignements qui forment des cas. Cela comprend l'établissement d'un calendrier ainsi que la coordination et l'exécution d'étapes de manière séquentielle ou parallèle pour accomplir une tâche. Cela comprend également le déclenchement d'événements (p. ex. notifications), la gestion des points où une tâche manuelle doit être effectuée par un utilisateur et la génération de listes des travaux aux fins d'examen.
Identification des logiciels malveillants	Cette composante analysera l'ensemble des observations – y compris les données importées à partir de supports physiques et de fichiers volumineux – à la recherche de contenu malveillant, cernera les observations potentiellement malveillantes et permettra d'examiner ces observations avant de poursuivre le traitement. Cette composante permet également de faire une comparaison entre des échantillons de logiciels malveillants fournis par des organismes canadiens d'application de la loi et figurant dans des solutions nationales et internationales choisies relatives aux logiciels malveillants.
Stockage des logiciels malveillants (objet)	Cette composante stocke l'échantillon de logiciel malveillant dans un environnement isolé ou de quarantaine, à part des autres fichiers qui sont traités par la solution. La solution doit se rapprocher le plus possible d'un isolement physique et faire en sorte que les échantillons de logiciels malveillants ne compromettent pas la sécurité ou l'intégrité du réseau de la GRC.
Modèles statistiques	Cette composante fournit une capacité avancée de faire de façon ponctuelle des analyses statistiques et de la modélisation de données.
Gestion des bibliothèques	Cette composante permet de gérer les versions des progiciels et des dépendances (p. ex. bibliothèques Python) pour l'élaboration et le déploiement dans l'environnement de science des données. Cette composante peut être une fonction de l'environnement de science des données ou être une composante à part.
Environnement de science des données	Cette composante fournit à l'utilisateur un environnement sûr, sécuritaire et isolé (p. ex. bac à sable) dans lequel appliquer des techniques et des outils avancés d'analyse. Elle permet aux utilisateurs de travailler dans des langages de science des données communs et populaires (p. ex. Python, Scala et Java), de documenter des techniques (p. ex. balisage), d'exécuter et de déployer des modèles et de visualiser des résultats, le tout dans un seul environnement (p. ex. bloc-notes).
Cyberoutils	Cette composante fournit aux utilisateurs un accès à divers cyberoutils (p. ex. dépistage de cryptomonnaies, recherche d'adresse IP, capture et analyse de paquets). Certains outils se trouvent sur les lieux, alors que d'autres sont offerts sous forme de SaaS.
Outils d'analyse visuelle	Cette composante permet de créer des graphiques et des diagrammes, d'analyser, d'étudier, de manipuler et de gérer des données. Les fonctions de visualisation permettent à l'utilisateur de prendre rapidement connaissance des données et peuvent comprendre des diagrammes de liens, des diagrammes d'événements, des cartes géospatiales et d'autres représentations graphiques (p. ex. StoryMaps) établis à partir de techniques d'analyse.

Tableau D-1 : Description des composantes de l'architecture

Composante architecturale	Description
Renseignement opérationnel	Cette composante fournit des fonctions automatisées d'analyse et de visualisation des données pour soutenir la prise de décisions. Elle établit des indicateurs de rendement et des indicateurs sommaires à partir des données et permet à l'utilisateur de prévoir la création automatique de rapports et de tableaux de bord en fonction de domaines d'intérêt prédéterminés.
Transcription	Cette composante transforme automatiquement en texte des fichiers audio.
Reconnaissance optique des caractères (ROC)	Cette composante extrait du texte à partir d'images qui contiennent du texte imprimé ou manuscrit.
Traduction	Cette composante permet de traduire du texte dans plusieurs combinaisons de langues. Au minimum, on l'utilise pour traduire du texte de l'anglais au français et vice versa.
Dépôt de données et base de connaissances du GNCC	Cette composante fournit un mécanisme central permettant de gérer l'ensemble des données opérationnelles du GNCC, y compris toutes les observations, les données brutes et nettoyées, les demandes de service, ainsi que toutes les métadonnées connexes et tous les artefacts numériques et produits opérationnels en découlant. Cela comprend un carrefour central de renseignements interrogeables sur des sujets et des techniques liés aux enquêtes sur la cybercriminalité.
Catalogue de données	Cette composante fournit des capacités pleinement automatisées et extensibles de gestion des métadonnées afin de permettre à l'utilisateur de découvrir rapidement et de gérer ses données. Elle rend automatique le suivi des objets dans l'unité de stockage des données à chaud (c.-à-d. objet) et dans l'unité de stockage des données à froid (c.-à-d. archives) et rend les métadonnées correspondantes facilement accessibles aux fins d'interrogation par l'entremise de la composante de recherche fédérée.
Stockage de données à chaud (objet)	Cette composante permet de stocker et de récupérer des données auxquelles on accède souvent en tant qu'objets dans n'importe quel format (p. ex. documents, images et fichiers audio/vidéo), avec un très faible temps d'attente.
Stockage de données à froid (archives)	Cette composante permet de stocker à long terme dans une base de données redondante des données auxquelles on n'accède pas fréquemment dans n'importe quel format (p. ex. documents, images et fichiers audio et vidéo) et de les récupérer.
Recherche fédérée	Cette composante permet à l'utilisateur de rechercher et de récupérer des renseignements dans des sources de données du GNCC sous une variété de formats, à l'aide d'une recherche unique. Une fonction de recherche avancée doit également être offerte pour permettre d'effectuer une recherche à facettes et d'accéder à du contenu en mode descendant.
Surveillance de la conformité	Cette composante gère les activités de données et en fait le suivi tout au long du cycle de vie des renseignements du GNCC (c.-à-d. de la réception/création à l'élimination/archivage) afin de garantir la conformité avec les normes et les politiques du gouvernement et de l'industrie.
Point d'application de la politique	Cette composante permet de gérer l'accès aux actifs d'information en fonction des rôles. Elle restreint l'accès aux fonctionnalités en fonction des attributs de l'utilisateur (p. ex. nom d'utilisateur, rôle ou territoire de compétence).

Tableau D-1 : Description des composantes de l'architecture

Composante architecturale	Description
Gestion de l'identité et de l'accès	Cette composante permet de gérer l'accès aux ressources – que ce soit par l'entremise d'interfaces Web ou par programmation – à l'aide de permissions et de politiques. Elle gère l'identité des utilisateurs (p. ex. noms d'utilisateur, mots de passe et clés d'accès), les rôles et les groupes, en plus de permettre la fédération d'identités et l'authentification à facteurs multiples (AFM).
Gestion des clés	Cette composante permet à l'utilisateur autorisé du GNCC de gérer la délivrance et la révocation de clés publiques et privées dans l'infrastructure à clés publiques qu'utilise la solution.
Gestion des journaux	Cette composante enregistre l'ensemble des activités des utilisateurs et du système dans des journaux d'activités accessibles en lecture seule afin de fournir un registre pouvant faire l'objet d'une vérification à des fins de conformité, de rendement, d'analyse et de sécurité.
Surveillance de la sécurité et du rendement	Cette composante fournit des capacités de surveillance du système en temps réel, y compris une surveillance des ressources et des réseaux du système. Elle fonctionne parallèlement à la composante de gestion des journaux afin d'analyser les journaux, de générer des indicateurs et d'envoyer des notifications aux administrateurs de système à l'aide de la composante de gestion des notifications.
Passerelle d'interface de programmation d'application (API)	Cette composante fournit une solution de gestion des API qui permet aux développeurs de créer, de publier, de maintenir, de surveiller et de sécuriser les API dans l'ensemble de la solution. Elle encourage le couplage lâche des composantes et soutient l'intégration avec les actifs organisationnels de la GRC ainsi qu'avec les systèmes de partenaires choisis, au moyen de normes ouvertes.
Service de liste d'attente	Cette composante fournit un service des messages en attente afin de soutenir la coordination souple des composantes, des listes des travaux en attente et des notifications. Elle fonctionne parallèlement à la composante de gestionnaire d'événements pour la gestion des déclencheurs et de la livraison des messages.
Gestionnaire des notifications	Cette composante fournit des fonctionnalités pour soutenir la gestion des notifications aux utilisateurs, y compris les listes des diffuseurs et des abonnés autorisés. Elle répond à des déclencheurs d'événements, tient compte des règles en matière de divulgation et affiche et gère les notifications à l'intention des utilisateurs visés. Elle fonctionne parallèlement au gestionnaire d'événements et au service de liste d'attente pour la gestion de l'envoi des notifications.
Gestionnaire d'événements	Cette composante gère de façon asynchrone l'ensemble des messages et des interactions entre les composantes de la solution, en fonction des déclencheurs d'événements. Elle fournit un mécanisme central pour garantir que les services sont coordonnés dans l'exécution de tâches complexes.
Courriels sécurisés	Cette composante permet de déchiffrer les courriels sécurisés reçus ainsi que de créer et d'envoyer des courriels sécurisés (c.-à-d. chiffrés) dans le P3 et dans le portail d'autres partenaires.
Connexion spécialisée au nuage	Cette composante fournit une connexion sécurisée, spécialisée et haute vitesse entre le centre de données de la GRC et l'espace infonuagique Protégé B de la GRC.

Tableau D-1 : Description des composantes de l'architecture

Composante architecturale	Description
Réseau privé virtuel (VPN)	Cette composante fournit un réseau sécurisé et privé de communication dans l'Internet public entre les ressources dans les locaux de la GRC et l'espace infonuagique Protégé B de la GRC.
Gestion des fichiers volumineux	Cette composante permet à la GRC et aux organisations partenaires de télécharger et de gérer de façon sécuritaire des fichiers volumineux dans un endroit accessible et sécuritaire.
Clavardage sécurisé (entre les pairs)	Cette composante permet aux utilisateurs du GNCC et du P3 de communiquer en temps réel et de façon sécuritaire en clavardant. Elle enregistre les utilisateurs qui ont participé à la séance ainsi que la date et l'heure de la séance de clavardage.

Appendice E – La matrice de traçabilité des exigences en matière de sécurité

a) La matrice de traçabilité des exigences de sécurité (SRTM) de la (SNC) énumère les contrôles de sécurité qui doivent être inclus dans la solution. Le tableau ci-dessous énumère l'identifiant du contrôle de sécurité (Nº) ainsi que le nom, la responsabilité du contrôle et la division de la responsabilité (si elle est partagée entre la GRC et l'entrepreneur en tant que contrôle à plusieurs parties). Pour plus de détails sur le contrôle, voir l'annexe 3A - Catalogue de contrôle de sécurité (ITSG-33) sur le site Web du Centre canadien pour la cybersécurité.

b) La colonne la plus à droite du tableau E-1, intitulée **Améliorations attribuées à l'entrepreneur**, énumère les améliorations de contrôle décrites dans le catalogue de contrôle de sécurité (ITSG-33) qui sont désignées comme étant réalisées par l'entrepreneur. Lorsqu'une amélioration est indiquée comme étant " partagée ", la GRC et l'entrepreneur se partagent la responsabilité de sa mise en œuvre.

Tableau E-1: Matrice de traçabilité des exigences en matière de sécurité

Nº	Nom	Responsabilités pour les contrôles SNC	Répartition des responsabilités pour les contrôles partagés en plusieurs parties	Améliorations attribuées à l'entrepreneur
AC-1	Politique et Procédures de Contrôle d'accès	Partagée		
AC-2	Gestion des comptes	Partagée		AC-2(1) - Partagée AC-2(2) - Partagée AC-2(3) - Partagée AC-2(4) - Partagée AC-2(5) - Partagée AC-2(7) – Partagée AC-2(9) – Partagée AC-2(10) – Partagée AC-2(11)

				AC-2(12) AC-2(13)
AC-3	Application De l'accès	Partagée		
AC-4	Application Du Contrôle De Flux d'information	Entrepreneur		AC-4(21)
AC-5	Séparation des tâches	Partagée	a) Partagée b) Entrepreneur c) Entrepreneur	
AC-6	Droit d'accès Minimal	Partagée		AC-6(1) – Partagée, AC-6(2) – Partagée AC-6(3) – Partagée AC-6(5) – Partagée AC-6(7) – Partagée AC-6(8) – Partagée AC-6(9) – Partagée AC-6(10) – Partagée
AC-7	Tentatives d'ouverture De Session Infructueuses	Partagée		
AC-8	Avis d'utilisation Système	Partagée		
AC-9	Avis d'ouverture De Session Précédente (Accès)	Entrepreneur		AC-9 (1)
AC-10	Contrôle De Sessions Simultanées	Partagée		
AC-11	Verrouillage De Session	Partagée		AC-11(1) - Partagée
AC-12	Fin De Session	Partagée		AC-12(1)
AC-14	Opérations permises sans identification ni authentification	Partagée		

AC-17	Accès a distance	Partagée		AC-17(1) AC-17(2) – Partagée AC-17(3) – Partagée AC-17(4), AC-17(9) AC-17(
AC-18	Accès sans fil	Partagée		AC-18(1) – Partagée AC-18(5)
AC-19	Contrôle d'accès Pour Les Dispositifs Mobiles	Partagée		AC-19(4) AC-19(5)
AC-20	Utilisation De Systèmes d'information Externes	Partagée		AC-20(1) – Partagée AC-20(2) - Partagée
AC-21	Collaboration Et Échange d'information Entre Utilisateurs	Partagée	A) Entrepreneur B) GRC	
AC-22	Contenu accessible au public	Partagée		
AC-23	Protection Contre l'exploration De Données	Entrepreneur		
AC-24	Décisions De Contrôle d'accès	Partagée		
AT-1	Politique et procédures de formation et de sensibilisation à la sécurité	Partagée		
AT-2	Sensibilisation à la sécurité	Partagée		AT-2(1) - Partagée AT-2(2) – Partagée
AT-3	Formation a la sécurité axée sur les rôles	Partagée		AT-3(1) AT-3(2) AT-3(3)
AT-4	Dossiers de formation a la sécurité	Partagée		

AU-1	Politique et procédures de vérification et de responsabilité	Partagée		
AU-2	Evénements vérifiables	Partagée	A) Entrepreneur B) GRC C) GRC D) GRC	AU-2(3) – Partagée
AU-3	Contenu des enregistrements de vérification	Partagée		AU-3(1) - Partagée AU-3(2) – Partagée
AU-4	Capacité de stockage des vérifications	Entrepreneur		
AU-5	Intervention En Cas d'échecs De Vérification	Partagée		AU-5(1) AU-5(2)
AU-6	Examen, analyse et rapports de vérification	Partagée		AU-6(1) – Partagée AU-6(3) – Partagée AU-6(10) – Partagée
AU-7	Réduction des vérifications et génération de rapports	Partagée		AU-7(1) – Partagée
AU-8	Estampilles temporelles	Entrepreneur		AU-8(1)
AU-9	Protection De l'information De Vérification	Partagée		AU-9(2) AU-9(3) AU-9(4) – Partagée
AU-10	Non-répudiation	Entrepreneur		
AU-11	Conservation des enregistrements de vérification	Partagée		
AU-12	Génération d'enregistrements De Vérification	Entrepreneur		AU-12(2)
AU-14	Vérification des sessions	Entrepreneur		AU-14(1)
CA-1	Politiques Et Procédures d'évaluation De Sécurité Et d'autorisation	Partagée		
CA-2	Évaluations de sécurité	Partagée	A) GRC	CA-2(1) – Partagée

			B) Partagée C) GRC D) GRC	CA-2(2) – Partagée CA-2(3)
CA-3	Connexions Des Systèmes d'information	Partagée		CA-3(3) – Partagée CA-3(5) – Partagée
CA-5	Plan d'action Et Jalons	Entrepreneur		
CA-6	Autorisation de sécurité	GRC		
CA-7	Surveillance continue	Partagée	A) GRC B) Entrepreneur pour l'outillage, GRC pour les opérations C) GRC D) GRC E) GRC F) GRC G) GRC	CA-7(1) – Partagée
CA-8	Tests de pénétration	Entrepreneur		CA-8(1)
CA-9	Connexions Des Systèmes d'information Internes	Partagée	A) GRC B) Entrepreneur	
CM-1	Politique et procédures de gestion des configurations	Partagée		
CM-2	Configuration de référence	Partagée		CM-2(1) – Partagée CM-2(2) – Partagée CM-2(7) – Partagée
CM-3	Contrôle des changements de configuration	Partagée	A) GRC B) GRC C) GRC	CM-3(1) - Partagée CM-3(4) CM-3(6)

			D) Entrepreneur E) Entrepreneur F) Partagée G) Partagée	
CM-4	Analyse concernant les répercussions sur la sécurité	Partagée		
CM-5	Restrictions d'accès Concernant Les Changements	Partagée		CM-5(1) CM-5(3) CM-5(5) - Partagée CM-5(6)
CM-6	Paramètres de configuration	Partagée	A) Entrepreneur B) Entrepreneur C) Partagée D) Partagée	CM-6(1) CM-6(2) - Partagée
CM-7	Fonctionnalité minimale	Entrepreneur		CM-7(1) - Partagée, CM-7(2) CM-7(5) - Partagée
CM-8	Inventaire Des Composants De Système d'information	Entrepreneur		CM-8(1) CM-8(2) CM-8(3) CM-8(5)
CM-9	Plan de gestion des configurations	Partagée		
CM-10	Restrictions Relatives A l'utilisation Des Logiciels	Partagée	A) Entrepreneur B) Entrepreneur C) S.O.	CM-10(1) - Partagée
CM-11	Logiciels Installés Par l'utilisateur	Partagée	A) GRC B) Entrepreneur C) GRC	
CP–1	Politique Et Procédures De Planification d'urgence	Partagée		

CP-2	Plan d'urgence	Partagée	A) Partagée a) GRC b) GRC c) GRC d) Entrepreneur e) Entrepreneur f) GRC B) Entrepreneur C) GRC D) Partagée E) Entrepreneur F) Entrepreneur G) Partagée	CP-2(1) - Partagée CP-2(2) CP-2(3) – Partagée CP-2(6) – Partagée CP-2(8) – Partagée
CP-3	Formation En Mesures d'urgence	Entrepreneur		
CP-4	Tests Et Exercices Relatifs Au Plan d'urgence	Partagée		CP-4(1) - Partagée
CP-6	Site de stockage de secours	Entrepreneur		CP-6(1) CP-6(3)
CP-7	Site de traitement de secours	Entrepreneur		CP-7(1) CP-7(2) CP-7(3) CP-7(4)
CP-8	Services de télécommunication	Entrepreneur		CP-8(1) CP-8(2) CP-8(3)
CP-9	Sauvegarde Du Système d'information	Partagée	A) Entrepreneur B) Entrepreneur C) Entrepreneur D) Entrepreneur AA) GRC	CP-9(1) - Partagée CP-9(3) - Partagée CP-9(5) CP-9(7) - Partagée

CP-10	Reprise Et Reconstitution Du Système d'information	Entrepreneur		CP-10(2) - Partagée
IA-1	Politique Et Procédures d'identification Et d'authentification	Partagée		
IA-2	Identification et authentification (utilisateurs organisationnels)	Entrepreneur		IA-2(1) IA-2(2) IA-2(3) IA-2(4) IA-2(5) IA-2(6) IA-2(8) IA-2(11)
IA-3	Identification et authentification des dispositifs	Entrepreneur		
IA-4	Gestion des identificateurs	Partagée	A) GRC B) GRC pour l'utilisateur ; Entrepreneur pour les comptes du système C) GRC pour l'utilisateur ; Entrepreneur pour les comptes du système D) GRC pour l'utilisateur ; Entrepreneur pour les comptes du système E) GRC	IA-4(4) – Partagée
IA-5	Gestion des authentifiants	Partagée		IA-5(1) – Partagée IA-5(2) – Partagée IA-5(3) – Partagée

				IA-5(4) – Partagée IA-5(6) – Partagée IA-5(7) – Partagée IA-5(11)
IA-6	Réinjection d'authentification	Entrepreneur		
IA-7	Authentification des modules cryptographiques	Entrepreneur		
IA-8	Identification et authentification (utilisateurs non organisationnels)	Entrepreneur		
IR-1	Politique Et Procédures d'intervention En Cas d'incident	Partagée		
IR-2	Formation Sur Les Interventions En Cas d'incident	Partagée		
IR-3	Tests Et Exercices Relatifs Aux Interventions En Cas d'incident	Entrepreneur		IR-3(2) - Partagée
IR-4	Traitement des incidents	Partagée	A) Partagée B) GRC C) GRC	IR-4(1)
IR-5	Surveillance des incidents	Entrepreneur		
IR-6	Signalement des incidents	Entrepreneur		IR-6(1)
IR-7	Assistance En Cas d'incident	Entrepreneur		IR-7(1) IR-7(2) - Partagée
IR-8	Plan d'intervention En Cas d'incident	Entrepreneur		
IR-9	Intervention En Cas De Fuite d'information	Partagée	A) GRC B) GRC C) Partagée D) Partagée E) GRC F) Partagée	IR-9(1) IR-9(2) IR-9(3) - Partagée IR-9(4) - Partagée

MA-1	Politique et procédures de maintenance des systèmes	Entrepreneur		
MA-2	Maintenance contrôlée	Partagée	A) Entrepreneur B) Partagée C) Partagée D) Entrepreneur E) Entrepreneur F) Entrepreneur	MA-2(2)
MA-3	Outils de maintenance	Entrepreneur		MA-3(1) MA-3(2) MA-3(3)
MA-4	Télémaintenance	Partagée	A) Partagée B) Entrepreneur C) Entrepreneur D) Entrepreneur	MA-4(1) MA-4(2) MA-4(3) MA-4(6) MA-4(7)
MA-5	Personnel de maintenance	Partagée		MA-5(1)
MA-6	Maintenance opportune	Entrepreneur		
MP-1	Politique et procédures de protection des supports	Entrepreneur		
MP-2	Accès aux supports	Entrepreneur		
MP-3	Marquage des supports	Entrepreneur		
MP-4	Entreposage des supports	Entrepreneur		
MP-5	Transport des supports	Partagée		MP-5(4)
MP-6	Nettoyage des supports	Entrepreneur		MP-6(1) MP-6(2)
MP-7	Utilisation des supports	Entrepreneur		MP-7(1)
PL-1	Politique et procédures de planification de la sécurité	Entrepreneur		

PL-2	Plan de sécurité du système	Partagée		PL-2(3) - Partagée
PL-4	Règles de conduite	Partagée	Partagée	PL-4(1)
PL-8	Architecture De Sécurité De l'information	Entrepreneur		
PS-1	Politique et procédures de sécurité du personnel	Partagée		
PS-2	Catégorisation des postes	Partagée		
PS-3	Enquête de sécurité sur le personnel	Partagée		PS-3(3) - Partagée
PS-4	Cessation d'emploi	Partagée		PS-4(2) - Partagée
PS-5	Transfert du personnel	Partagée		
PS-6	Ententes d'accès	Partagée		
PS-7	Sécurité du personnel de tierces parties	Partagée		
PS-8	Sanctions imposées au personnel	Partagée		
RA-1	Politique Et Procédures d'évaluation Des Risques	Partagée		
RA-2	Catégorisation de sécurité	Partagée		
RA-3	Évaluation des risques	Partagée		
RA-5	Analyse des vulnérabilités	Entrepreneur		RA-5(1) RA-5(2) RA-5(3) RA-5(5) RA-5(6) RA-5(8)
SA-1	Politique Et Procédures d'acquisition Des Systèmes Et Des Services	Entrepreneur		
SA-2	Affectation des resources	Entrepreneur		
SA-3	Cycle de développement de système	Entrepreneur		

SA-4	Processus d'acquisition	Entrepreneur		SA-4(1) SA-4(2) SA-4(3) SA-4(7) SA-4(8)
SA-5	Documentation Relative Aux Systèmes d'information	Entrepreneur		
SA-8	Principes d'ingénierie De Sécurité	Entrepreneur		
SA-9	Services De Système d'information Externes	Entrepreneur		SA-9(1) SA-9(2) SA-9(4) SA-9(5) (résidence de l'information)
SA-10	Gestion des configurations par les développeurs	Entrepreneur		SA-10(1)
SA-11	Tests de sécurité effectués par les développeurs	Entrepreneur		SA-11(1) SA-11(2) SA-11(8)
SA-12	Protection De La Chaîne d'approvisionnement	Entrepreneur		SA-12(1) SA-12(2) SA-12(5) SA-12(7) SA-12(8) SA-12(9) SA-12(11)
SA-14	Analyse de criticité	Entrepreneur		
SA-15	Processus de développement, normes et outils	Entrepreneur		
SA-16	Formation offerte par le développeur	Entrepreneur		
SA-17	Architecture et conception de sécurité du développeur	Entrepreneur		

SA-21	Sélection des développeurs	Partagée		
SC-1	Politique et procédures de protection des systèmes et des communications	Entrepreneur		
SC-2	Partitionnement des applications	Entrepreneur		
SC-3	Isolement des fonctions de sécurité	Entrepreneur		
SC-4	Information contenue dans les ressources partagées	Entrepreneur		
SC-5	Protection contre les dénis de service	Entrepreneur		
SC-6	Disponibilité des ressources	Entrepreneur		
SC-7	Protection des frontières	Partagée		SC-7(3) SC-7(4) SC-7(5) SC-7(7) SC-7(8) SC-7(10) SC-7(12) SC-7(13) SC-7(14) SC-7(18) SC-7(19) SC-7(21) - Partagée
SC-8	Confidentialité et intégrité des transmissions	Partagée		SC-8(1) - Partagée
SC-10	Déconnexion réseau	Entrepreneur		
SC-12	Établissement et gestion des clés cryptographiques	Partagée		SC-12(2) - Partagée SC-12(3) - Partagée
SC-13	Protection cryptographique	Entrepreneur		
SC-15	Dispositifs d'informatique Coopérative	Entrepreneur		

SC-17	Certificats d'infrastructure À Clé Publique	Partagée		
SC-18	Code mobile	Partagée	A) GRC B) GRC C) Entrepreneur	SC-18(3) SC-18(4)
SC-19	Voix sur protocole internet	Partagée	A) GRC B) Entrepreneur	
SC-20	Service Sécurisé De Résolution De Nom Ou d'adresse (Source Autorisée)	Entrepreneur		
SC-21	Service Sécurisé De Résolution De Nom Ou d'adresse (Résolveur Récursif Ou Cache)	Entrepreneur		
SC-22	Architecture Et Fourniture De Services De Résolution De Nom Ou d'adresse	Entrepreneur		
SC-23	Authenticité des sessions	Entrepreneur		SC-23(1)
SC-28	Protection De l'information Inactive	Entrepreneur		SI-28(1)
SC-39	Isolement des processus	Entrepreneur		
SC-43	Restrictions Concernant l'utilisation	Entrepreneur		
SI-1	Politique Et Procédures Liées À l'intégrité De l'information Et Des Systèmes	Entrepreneur		
SI-2	Correction des défauts	Entrepreneur		SI-2(1) SI-2(2) SI-2(3)
SI-3	Protection contre les codes malveillants	Entrepreneur		SI-3(1) SI-3(2) SI-3(7)
SI-4	Surveillance Des Systèmes d'information	Entrepreneur		SI-4(1) SI-4(2)

				SI-4(4) SI-4(5) SI-4(7) SI-4(11) SI-4(14) SI-4(16) SI-4(20) SI-4(22) SI-4(23)
SI-5	Alertes, avis et directives de sécurité	Partagée		SI-5(1)
SI-6	Vérification de la fonctionnalité de sécurité	Entrepreneur		
SI-7	Intégrité Des Logiciels, Des Micro logiciels Et De l'information	Entrepreneur		SI-7(1) SI-7(5) SI-7(7)
SI-8	Protection Anti pourriel	Entrepreneur		SI-8(1) SI-8(2)
SI-10	Validation De La Saisie d'information	Entrepreneur		
SI-11	Traitement des erreurs	Entrepreneur		
SI-12	Traitement Et Conservation Des Sorties d'information	Entrepreneur		
SI-15	Filtrage Des Sorties d'information	Entrepreneur		
SI-16	Protection de la mémoire	Entrepreneur		

Appendice F – Données volumétriques

Le tableau ci-dessous contient les données volumétriques de la SNC estimées en fonction de la solution utilisée par les partenaires de l'application de la loi et de la cybercriminalité.

Tableau F-1 : Croissance estimée des données sur une année

	Notes sur les types de transaction	Volume estimé des opérations (par an)	Téraoctets estimés (par an)
A	Demandes de service incluant demandes d'information, de conseil et d'orientation, d'accès à la base de connaissances, demandes d'information spéciales, dépôts de données, opérations de coordination et demandes de conversation de données. Taille moyenne des transactions estimée à 5 Ko.	725,000	3.4
B	Dépôt de données aux fins d'analyse, de réponse ou d'ajout aux données du GNCC – chaque volume estimé à 500 Ko ou moins (p. ex. enquêtes liées à la cybercriminalité, analyse des renseignements sur la cybercriminalité, dépôts de données au GNCC [partage des données]).	15,000	0.007
C	Dépôts de données représentant 5 Go. Volume représentant environ 1 200 opérations par année. Demandes d'analyse, de réponse ou d'ajout aux donnes du GNCC. Dépôts d'au plus 5 Go.	1,200	5.9
D	Dépôts de données d'enquête majeure (20 To chaque) aux fins d'analyse, de réponse ou d'ajout aux données du GNCC. Les soumissions d'enquêtes majeures peuvent s'élever à 20 To, mais ils peuvent aussi fluctuer beaucoup. Les dépôts seront probablement réalisés par ingestion au moyen d'un transfert de gros fichier ou d'un support physique. L'extensibilité est essentielle pour traiter de tels volumes.	5	97.6
E	Plaintes du public (p. ex. signalements de cyberattaque ou de fraude reçus par le truchement du site Web du système de signalement des incidents de cybercriminalité et de fraude). Ce sont pour la plupart des données d'environ 1 Ko, et il est possible d'y joindre des images. L'estimation des données prévoit que 15 % des dépôts incluent une image de 250 Ko.	160,000	0.006
F	Flux de renseignements liés à la cybercriminalité et à diverses menaces et projets spéciaux représentant un volume total d'environ 5 To par année. De façon périodique, la SNC ingérera divers flux de données diverses liées à la cybercriminalité et au renseignement. Il peut s'agir de grands flux de données contenant des extraits de sites Web, des données MISP et d'autres données de renseignement sur des menaces qui seront utilisés aux fins d'analyse et de mises en corrélation. Les types et les volumes de données varies, mais les gros ensembles de données sont	S.O.	4.9

	courants. Les données sont tirées de sources ouvertes et de sources privées de renseignements sur les menaces liées à la cybercriminalité.		
		Total	**111.8**

Le tableau ci-dessous présente la croissance estimée des données volumétriques sur une année.

Tableau F-2: **C**roissance estimée des données volumétriques sur une année

Tableau F-1 reference	Année 1	Année 2	Année 3	Année 4	Année 5	Année 6	Année 7	Année 8
A	616,250	688,750	761,250	797,500	833,750	841,000	848,250	855,500
B	12,750	14,250	15,750	16,500	17,250	17,400	17,550	17,700
C	1,020	1,140	1,260	1,320	1,380	1,392	1,404	1,416
D	4	5	5	6	6	6	6	6
E	160,000	171,200	172,800	186,624	201,554	217,678	235,092	253,900

Le tableau ci-dessous présente la croissance estimée du Dépôt de données de la SNC et du nombre d'utilisateurs de la SNC sur une année.

Année de projet	Année 1	Année 2	Année 3	Année 4	Année 5	Année 6	Année 7	Année 8
Total des téraoctets accumulés sur une année	103	230	377	537	710	890	1,070	1,250
Utilisateurs internes (ajoutés)	170	150	100	20	20	20	20	20
Utilisateurs externes (ajoutés)	200	700	600	75	75	75	75	75

Appendice G – Tableaux de référence pour le modèle de services infonuagiques

1. L'objet du présent appendice est de fournir aux soumissionnaires un cadre de référence dans lequel ils sont invités à décrire en détail les services et les ressources infonuagiques qu'ils proposent (selon la documentation sur l'architecture de système fournie à la Section 4.1 – Exigences générales. Ce cadre comprend :

    a. un tableau de l'ensemble des services et des ressources infonuagiques que l'entrepreneur demande à la GRC de fournir afin de pouvoir déployer sa solution et fournir le soutien nécessaire;

    b. un tableau de tous les autres services et ressources infonuagiques proposés.

2. Les entrepreneurs qui proposent une solution pour laquelle la GRC devra s'approvisionner en services et ressources infonuagiques (dans le cas où l'ensemble ou une partie de la solution est hébergée dans l'espace infonuagique de la GRC [IaaS ou PaaS privée]) avec octroi de licences perpétuelles doivent remplis les sections applicables du Tableau G 1 : Ressources infonuagiques que la GRC doit fournir. Il faut suivre les instructions suivantes :

    a. indiquer le fournisseur de services infonuagiques;

    b. inclure une brève description de chaque service ou ressource infonuagique que la GRC hébergera dans son espace infonuagique et préciser la page ou l'endroit où se trouvent les détails pertinents dans la section sur le modèle de services infonuagiques de l'entrepreneur de la documentation sur l'architecture de solution proposée;

    c. fournir à l'autorité technique tous les renseignements dont elle a besoin pour calculer auprès d'un fournisseur de services infonuagiques le coût approximatif des ressources infonuagiques que la GRC devra fournir pour que la solution proposée puisse être prise en charge;

    d. utiliser les termes employés par le fournisseur de services infonuagiques pour décrire les services et les ressources infonuagiques pertinents, y compris *les types et les tailles*;

    e. préciser la page ou la section de la documentation sur l'architecture du système (voir la Section 4.1 – Exigences générales) qui traite de l'environnement virtuel, de la taille, de l'élasticité, de l'extensibilité, de la haute disponibilité et de la résilience de la ressource, de la croissance des données sur 10 ans, etc.

    f. fournir tous les renseignements dont la GRC a besoin pour calculer auprès d'un fournisseur de services infonuagiques le coût des services ou des ressources infonuagiques hébergera dans son espace infonuagique.

2. Les entrepreneurs qui proposent une solution intégrant un SaaS ou une PaaS publique doivent remplir le Tableau G 2 : Ressources infonuagiques pour la solution – SaaS et PaaS publique et :

    a. mentionner si le service répond aux exigences de la DAMA-SaaS ou non;

    b. mentionner si le service est approuvé à titre de service de courtage infonuagique du GC (SPC) pour un usage protégé B;

    c. préciser la page ou la section de la documentation sur l'architecture du système où il est question du SaaS ou de la PaaS pour faciliter la mise en contexte et en savoir plus sur l'élasticité, l'extensibilité et la résilience du service, la croissance des données sur 10 ans, etc.

Tableau G-1 : Ressources infonuagiques que la GRC doit fournir

Solution exigeant que la GRC possède des ressources infonuagiques				
Fournisseur de services infonuagiques :				
N^bre^	**Catégorie de service infonuagique**	**Nom du service et brève description**	**Renvoi à la page ou à la section du document sur l'architecture du système – modèle de services infonuagiques**	**Éléments d'architecture concernés**
1	*Ordinateur*	**Exemple :** *N^bre^ de machines virtuelles ou d'environnements EC2, haute disponibilité, région, etc.* *Référence au numéro du fournisseur de services infonuagiques pour le service ou la ressource, à l'UGS, etc.*	*Voir la proposition technique – Architecture du système – modèle de services infonuagiques, section 4.x.x*	*- Machines virtuelles* *- Environnements ordinateur* *- Haute disponibilité*
	Stockage des données			
	Réseau			
	Surveillance et gestion			

Tableau G-1 : Ressources infonuagiques que la GRC doit fournir

Solution exigeant que la GRC possède des ressources infonuagiques				
Fournisseur de services infonuagiques :				
N^bre^	**Catégorie de service infonuagique**	**Nom du service et brève description**	**Renvoi à la page ou à la section du document sur l'architecture du système – modèle de services infonuagiques**	**Éléments d'architecture concernés**
	Autre			

Tableau G-2 : Ressources infonuagiques pour la solution – SaaS et PaaS publique

Sommaire du modèle de services infonuagiques – SaaS ou PaaS publique					
N^bre^	**Nom du SaaS ou de la PaaS publique et adresse URL vers le SaaS**	**Nom du fournisseur de services infonuagiques**	**Renvoi à la page ou à la section du document sur l'architecture du système – modèle de services infonuagiques**	**Répond aux exigences de niveau 2 de la DAMA-SaaS**	**Approuvé au titre du Catalogue de services de courtage infonuagique GC (protégé B) de SPC**

Tableau G-2 : Ressources infonuagiques pour la solution – SaaS et PaaS publique

Sommaire du modèle de services infonuagiques – SaaS ou PaaS publique					
N^bre	**Nom du SaaS ou de la PaaS publique et adresse URL vers le SaaS**	**Nom du fournisseur de services infonuagiques**	**Renvoi à la page ou à la section du document sur l'architecture du système – modèle de services infonuagiques**	**Répond aux exigences de niveau 2 de la DAMA-SaaS**	**Approuvé au titre du Catalogue de services de courtage infonuagique GC (protégé B) de SPC**

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915/C	-	155 XL
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
M7594-205915	155xl M7594-205915	

ANNEXE B

BASE DE PAIEMENT

Les soumissionnaires sont tenus d'utiliser les tableaux de prix ci-dessous pour soumettre leur soumission financière.

TABLEAU DE PRIX 1 (TP1)		
PROTOTYPE DE SOLUTION POUR L'ÉVALUATION DES CAPACITÉS ET DE LA CONVIVIALITÉ (ECC)		
Prix ferme tout compris en dollars canadiens (taxes applicables en sus) pour les travaux décrits dans la première phase : Prototype de solution de l'Énoncé des travaux à l'annexe A, qui comprend l'octroi de tous les droits d'utilisation de la solution, les octrois d'accès, la documentation du logiciel, la garantie, la formation virtuelle sur l'utilisation du prototype, la maintenance ainsi que le soutien, les renonciations, les ententes de non-divulgation et tout autre lancement destiné au Canada en vue de mener l'ECC, l'objectif étant de permettre à un maximum de 100 utilisateurs d'utiliser la solution prototype pour l'ECC pendant la durée initiale du contrat.		
Article no (A)	**Description (B)**	**Prix de lot ferme tout compris (C)**
1	Tous les produits livrables associés à la première phase, y compris le prototype de solution, conformément à l'annexe A – Énoncé des travaux.	$ 200 000
TP1 : Prix total évalué de la soumission (somme de la colonne [C])		**$ 200 000**

TABLEAU DE PRIX 2 (TP2)		
TEST DU PROTOTYPE SUR PLATEFORME (le cas échéant)		
Prix ferme tout compris en dollars canadiens (taxes applicables en sus) pour l'installation et le déploiement réussis de la solution prototype de l'entrepreneur, le cas échéant, conformément au modèle de déploiement infonuagique Protégé B de l'entrepreneur défini à l'annexe A de l'Énoncé des travaux, y compris, sans s'y limiter, l'octroi de tous les droits d'utilisation de la solution, les octrois d'accès, la documentation sur le logiciel, la garantie, la maintenance et le soutien (à l'exclusion de la formation), les renonciations, les ententes de non-divulgation et tout autre lancement destiné au Canada, aux fins de la réalisation du test du prototype sur plateforme pour un maximum de 100 utilisateurs autorisés.		
Article no (A)	**Description (B)**	**Prix de lot ferme tout compris (C)**
1	Réussite du test du prototype sur plateforme conformément à l'annexe A – Énoncé des travaux.	$ 25 000
TP2 : Prix total évalué de la soumission (somme de la colonne [C])		**$ 25 000**
Note: Le test POP peut être effectué à la seule discrétion du Canada.		

INSTRUCTIONS AUX SOUMISSIONNAIRES POUR LE TABLEAU 3
Les soumissionnaires sont tenus de remplir le tableau de mise en œuvre des solutions pour leur solution conformément au plan de mise en œuvre figurant à l'Annexe A – Énoncé des travaux.

TABLEAU DE PRIX 3 (TP3)

MISE EN ŒUVRE DE LA SOLUTION

Prix ferme tout compris en dollars canadiens (taxes applicables en sus) pour la prestation de la solution complète (quel que soit le modèle visé : sur place, hybride ou SaaS) avec la fonctionnalité décrite à l'Annexe A – Énoncé des travaux. Comprend la planification de la solution, le soutien à la mise en œuvre (le cas échéant), le soutien à l'intégration (le cas échéant), la configuration, la formation, le matériel de formation mis à jour, la création et la tenue à jour de la formation en ligne, la garantie (le cas échéant), les renonciations, les ententes de non-divulgation et les autres versions au Canada.

N° d'article (A)	**Description (B)**	**Prix de lot ferme tout compris (C)**
1	Livraison de la solution du SNC	_____$
TP3 : Prix total évalué de la soumission (somme de (C))		**$**

INSTRUCTIONS AUX SOUMISSIONNAIRES POUR LE TABLEAU 4
Les soumissionnaires sont tenus de fournir des prix pour tous les articles appropriés qui correspondent à leur modèle de prestation de solutions et conformément à l'Annexe A – Énoncé des travaux. Si leur solution comporte à la fois des approches de licence perpétuelle ET d'accès des utilisateurs, le soumissionnaire doit ajouter des prix dans les deux lignes (#a et #b). Si un seul article (approche) est requis, soit #a ou #b, le soumissionnaire doit ajouter 0,00 à chaque article dont le prix n'est pas requis.

TABLEAU DE PRIX 4 (TP4)

OCTROI POUR
LICENCES D'UTILISATION SUPPLÉMENTAIRES (le cas échéant) OU
ACCÈS EN LIGNE POUR LES UTILISATEURS SUPPLÉMENTAIRES (le cas échéant) OU
LICENCES D'UTILISATION et ACCÈS EN LIGNE POUR LES UTILISATEURS SUPPLÉMENTAIRES (le cas échéant)
PENDANT LA MISE EN ŒUVRE DE LA SOLUTION

Prix ferme tout compris en dollars canadiens (taxes applicables en sus)

Article #a - #b (A)	Description (B)	Prix par utilisateur (C)	Nombre d'utilisateurs (D)	Prix calculé pour fins d'évaluation (E) = ((C) X (D))
1a	Licences d'utilisation conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
1b	Accès des utilisateurs conformément à l'Annexe A – Énoncé des travaux	_____ $	100	_____ $
TP4 Prix total évalué de la soumission (somme des prix en (E))				_____ $

Remarque : Aux fins de l'évaluation, 100 représente le nombre estimatif d'utilisateurs par période.

INSTRUCTIONS AUX SOUMISSIONNAIRES POUR LES TABLEAUX 5A ET 5B
Les soumissionnaires sont tenus de fournir des prix pour tous les articles appropriés qui correspondent à leur modèle de prestation de solutions et conformément à l'Annexe A – Énoncé des travaux. Si leur solution comporte à la fois des approches de licence d'utilisateur ET d'accès utilisateur, le soumissionnaire doit ajouter des prix dans les deux tableaux (TP5A et TP5B). Si un seul tableau (approche) est requis, à savoir TP5A ou TP5B, le soumissionnaire doit ajouter 0,00 à chaque article du tableau où le prix n'est pas requis.

TABLEAU 5A (TP5A)

OCTROI OPTIONNEL PAR LICENCE D'UTILISATEUR SUPPLÉMENTAIRE (le cas échéant)

Prix ferme tout compris en dollars canadiens (taxes applicables en sus)

Article (A)	Description (B)	Prix par utilisateur supplémentaire (C)	Utilisateurs supplémentaires (D)	Prix calculé pour des fins d'évaluation (E) = ((C) X (D))
1	Année d'option 1 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
2	Année d'option 2 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
3	Année d'option 3 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
4	Année d'option 4 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
5	Année d'option 5 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
6	Année d'option 6 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
7	Année d'option 7 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
8	Année d'option 8 : Licences d'utilisation supplémentaires conformément à l'Annexe A-Énoncé des travaux	_____ $	100	_____ $
TP5A : Prix total évalué de la soumission (somme des prix en (E) ÷ 8)				_____ $

Remarque : Aux fins de l'évaluation, 100 est le nombre estimatif d'utilisateurs supplémentaires par période.

TABLEAU 5B (TP5B)									
OCTROI OPTIONNEL POUR ACCÈS UTILISATEURS SUPPLÉMENTAIRES (le cas échéant)									
Prix ferme tout compris en dollars canadiens (taxes applicables en sus) pour accès utilisateurs supplémentaires à la solution hébergée capable de traiter les volumes de transaction décrits									
Nº d'article	**Volume de traitement de transactions**	**Prix ferme tout compris par lot de volume de transaction pour 100 accès utilisateurs supplémentaires par période optionnelle (PO)**							**Prix calculé aux fins de l'évaluation**
		PO 1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**	**(G)**	**(H)**	**(I)**	**(J)**	**Σ(C,…,J) (L)**
1	1 à 250 000	___ $	___ $	___ $	___ $	___ $	___ $	___ $	___ $	_____ $
2	250 001 à 500 000	___ $	___ $	___ $	___ $	___ $	___ $	___ $	___ $	_____ $
3	500 001 à 750 000	___ $	___ $	___ $	___ $	___ $	___ $	___ $	___ $	_____ $
4	750 001 à 1 000 000	___ $	___ $	___ $	___ $	___ $	___ $	___ $	___ $	_____ $
5	1 000 001 à 1 250 000	___ $	___ $	___ $	___ $	___ $	___ $	___ $	___ $	_____ $
6	Plus de 1 250 000	___ $	___ $	___ $	___ $	___ $	___ $	___ $	___ $	_____ $
TP5B : Prix total évalué de la soumission (somme des prix en (L) ÷ 8))										_____ $
Remarque : Aux fins de l'évaluation, 100 est le nombre estimatif d'utilisateurs supplémentaires par période.										

INSTRUCTIONS AUX SOUMISSIONNAIRES POUR LE TABLEAU 6			
Les soumissionnaires sont tenus de fournir des prix pour tous les articles appropriés qui correspondent à leur modèle de prestation de solutions. Si leur solution comprend des services de soutien et de maintenance ET des services d'hébergement et de soutien connexe, le soumissionnaire doit ajouter des prix dans les deux lignes (#a et #b). Si un seul ensemble d'articles est requis, soit #a ou #b, le soumissionnaire doit ajouter 0,00 à chaque article pour lequel aucun prix n'est requis.			
TABLEAU DE PRIX 6 (TP6)			
SERVICES OPTIONNELS: SERVICES DE MAINTENANCE ET DE SOUTIEN DE LA SOLUTION (le cas échéant) OU SERVICES D'HÉBERGEMENT DU SNC ET DE SOUTIEN CONNEXES A L'HÉBERGEMENT (le cas échéant) OU SERVICES DE MAINTENANCE ET DE SOUTIEN DE LA SOLUTION et SERVICES D'HÉBERGEMENT DU SNC ET SERVICES DE SOUTIEN CONNEXES À L'HÉBERGEMENT (le cas échéant)			
Prix ferme tout compris en dollars canadiens (taxes applicables en sus)			
Article #a - #b (A)	**Description** Pour la prestation de services de maintenance et de soutien du SNC ou de services d'hébergement et de soutien connexes à l'hébergement du SNC ou pour une combinaison d'ensembles de services antérieurs pendant la période d'option (PO), le cas échéant. **(B)**	**Prix total (C)**	**Prix annuel total (#a + #b) (D)**
1a	PO 1 : Services de maintenance et de soutien de la solution	_____ $	_____ $
1b	PO 1 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
2a	PO 2 : Services de maintenance et de soutien de la solution	_____ $	_____ $
2b	PO 2 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
3a	PO 3 : Services de maintenance et de soutien de la solution	_____ $	_____ $
3b	PO 3 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
4a	PO 4 : Services de maintenance et de soutien de la solution	_____ $	_____ $
4b	PO 4 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
5a	PO 5 : Services de maintenance et de soutien de la solution	_____ $	_____ $
5b	PO 5 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
6a	PO 6 : Services de maintenance et de soutien de la solution	_____ $	_____ $
6b	PO 6 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
7a	PO 7 : Services de maintenance et de soutien de la solution	_____ $	_____ $
7b	PO 7 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
8a	PO 8 : Services de maintenance et de soutien de la solution	_____ $	_____ $
8b	PO 8 : Hébergement du SNC et services de soutien connexes à l'hébergement	_____ $	
TP6 : Prix total évalué de la soumission (somme de tous les prix en (D))			_____ $

INSTRUCTIONS AUX SOUMISSIONNAIRES POUR LE TABLEAU 7
Les soumissionnaires sont tenus d'indiquer **toutes** les catégories de services professionnels (B) requises, avec les tarifs journaliers (C-J) et les prix totaux moyens (K) pour leur solution pendant chaque période d'option.

TABLEAU DE PRIX 7 (TP7)

SERVICES PROFESSIONNELS FACULTATIFS

Tarifs journaliers fermes tout compris en dollars canadiens (taxes applicables en sus) pour les services professionnels (SP) facultatifs qui seront fournis sur demande, tel que décrit à l'Annexe A – Énoncé des travaux et conformément au processus d'autorisation de tâches

N° d'article	Description de la catégorie de SP	Tarif journalier ferme tout compris par période d'option (PO)								Prix moyen calculé par période par SP : Σ(C,D,...,J) X 100 ÷ 8
		PO 1 tarif journalier	PO 2 tarif journalier	PO 3 tarif journalier	PO 4 tarif journalier	PO 5 tarif journalier	PO 6 tarif journalier	PO 7 tarif journalier	PO 8 tarif journalier	
(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)
1										
2										
3										
4										
5										
TP7 : Prix total évalué de la soumission (somme de tous les prix (K) ÷ (nombre total de catégories))										

Remarques : Aux fins de l'évaluation, 100 représente le niveau d'effort estimatif en jours pour chaque catégorie et chaque période. Un prix total évalué de la soumission, calculé en fonction du nombre de catégories, permet au soumissionnaire de fournir n'importe quel nombre de catégories de SP prévisibles requises pendant les périodes d'option sans être désavantagé dans le cadre de l'évaluation financière.

INSTRUCTIONS AUX SOUMISSIONNAIRES CONCERNANT LE TABLEAU 8
Les soumissionnaires sont tenus de remplir le tableau ci-dessous et d'ajouter toute autre catégorie de formation requise (B) et d'indiquer le prix par individu en formation (C-J) et les moyennes de prix par individu en formation (K) par catégorie pour leur solution pendant les périodes d'option.

TABLEAU DE PRIX 8 (TP8)

SERVICES DE FORMATION OPTIONNELLE

Prix ferme tout compris en dollars canadiens (taxes applicables en sus) par utilisateur pour la formation des Services de formation virtuels au fur et à mesure des besoins, tel que décrit à l'Annexe A – Énoncé des travaux et conformément au processus d'autorisation de tâches

Nº d'article	Description de la catégorie de formation	Prix ferme tout compris par individu en formation pendant la période d'option (PO)								Prix moyen prolongé par période pour 100 individus en formation : Σ(C,D,…,J) X 100 ÷ 8
		PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	
(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)
1	Utilisateur final									
2	Grand utilisateur									
3	Utilisateur expert en la matière									
4	Utilisateur du soutien technique									
5										
6										
TP8 : Prix total évalué de la soumission (somme de tous les prix (K) ÷ (nombre total de catégories))										

Remarques : Aux fins de l'évaluation, 100 représente le nombre estimatif d'individus en formation pour chaque période d'option. Un prix total évalué de la soumission calculé en fonction du nombre de catégories permet au soumissionnaire de fournir toute catégorie de formation prévisible requise pendant les périodes d'option sans être désavantagée dans le cadre de l'évaluation financière.

Prix total évalué de la soumission pour calculer la note financière = Σ (TP1, TP2, …, TP8)

TABLEAU DES PAIEMENTS D'ÉTAPE		
SOUTIEN À LA MISE EN ŒUVRE		
Article # (A)	**Description (B)**	**Tout inclus Prix de lot (C)**
1	Étape 1 • Selon le calendrier de mise en œuvre convenu • Fonctionnalité de gestion du contrôle opérationnel acceptée (conformément au plan de mise en œuvre convenu)	5 %
2	Étape 2 • Selon le calendrier de mise en œuvre convenu • Fonctionnalité de gestion du contrôle opérationnel acceptée (conformément au plan de mise en œuvre convenu)	10 %
3	Étape 3 • Selon le calendrier de mise en œuvre convenu • Fonctionnalité de gestion du contrôle opérationnel acceptée (conformément au plan de mise en œuvre convenu)	10 %
4	Étape 4 • Selon le calendrier de mise en œuvre convenu • Fonctionnalité de gestion du contrôle opérationnel acceptée (conformément au plan de mise en œuvre convenu)	10 %
5	Étape 5 • Selon le calendrier de mise en œuvre convenu • Fonctionnalité de gestion du contrôle opérationnel acceptée (conformément au plan de mise en œuvre convenu)	10 %
6	Étape 6 • Selon le calendrier de mise en œuvre convenu • Fonctionnalité de gestion du contrôle opérationnel acceptée (conformément au plan de mise en œuvre convenu)	20 %
7	Étape 7 • Selon le calendrier de mise en œuvre convenu • Livraison de la solution définitive de capacité opérationnelle acceptée	35 %
Prix total de mise en œuvre en pourcentage		100 %
Remarque : Ces pourcentages sont déterminés par le Canada, à sa seule discrétion.		

ANNEXE C

LISTE DE VÉRIFICATION DES EXIGENGES RELATIVES À LA SÉCURITÉ – PHASE 1 - PROTOTYPE

SRCL# 20201119075 - PROTOTYPE

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915 / M7594-205915
Security Classification / Classification de sécurité PROTECTED A

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
RCMP	IM/IT - NHQ / CIO / SDPPM
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

The work to be performed is for the prototyping of a National Cybercrime IM/IT Solution. An agile procurement process will be used, which includes the award of (3) prototype contracts to (3) different vendors, prior to issuance of the contract for the final solution. The prototype contracts will enable to assess the functionality of solution that is being proposed by the 3 vendors. Vendors' personnel will not require access to ROSS or to RCMP data during the prototype phase.

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

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

Canada ☐	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☐ Not releasable / À ne pas diffuser ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	All NATO countries / Tous les pays de l'OTAN ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	No release restrictions / Aucune restriction relative à la diffusion ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ☐	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☐	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915 / M7594-205915
Security Classification / Classification de sécurité
PROTECTED A

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

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

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

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

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

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

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

Special comments: ON SITE - Facility Access II with escort - Accès aux installations II avec escorte
Commentaires spéciaux : OFF SITE - Facility Access II without escort - Accès aux installations II sans escorte

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915 / M7594-205915
Security Classification / Classification de sécurité
PROTECTED A

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

☐ No / Non ☑ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915/ M7594-205915
Security Classification / Classification de sécurité
PROTECTED A

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Dusan Musal	Director	Digitally signed by Musal,Dusan,000169308 Date: 2020.04.27 12:02:20 -04'00'	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613-998-7329		Dusan.Musal@rcmp-grc.gc.ca	2020/04/27

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sheila Nordskog	Security Analyst		
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613-843-5247	613-823-0143	sheila.nordskog@rcmp-grc.gc.ca	2020-07-29

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

☐ No / Non ☑ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Mary Rutledge	A/Manager - Procurement Special Projects	Mary Rutledge	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
343-552-2386 / 613-843-6935		mary.rutledge@rcmp-grc.gc.ca	2020/05/15

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

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

Guide de sécurité – Liste de vérification des exigences relatives à la sécurité (LVERS)

Solution nationale en matière de cybercriminalité – Prototype
LVERS nº 20201119075

Préparé par :
Section centrale de la sécurité ministérielle
Gendarmerie royale du Canada

Exigences générales de sécurité

Tous les entrepreneurs engagés dans le cadre du contrat visé par le présent guide sont tenus de collaborer au maintien de l'environnement de sécurité de la GRC en se conformant aux directives énoncées ci-après.

1. Tous les renseignements protégés (documents papier) et autres biens de nature délicate dont la GRC est responsable doivent être transmis à l'entrepreneur suivant des processus approuvés préalablement.

2. Les renseignements communiqués par la GRC doivent être gérés, tenus à jour et éliminés conformément aux clauses du contrat. À tout le moins, l'entrepreneur est tenu de respecter la Politique sur la sécurité du gouvernement.

3. L'entrepreneur doit aviser promptement la GRC de toute utilisation ou divulgation non autorisée de l'information communiquée en vertu du contrat visé par le présent guide et il doit transmettre à la GRC les détails de l'utilisation ou de la divulgation non autorisée (p. ex. en cas de perte, accidentelle ou délibérée, de renseignements de nature délicate).

4. La prise de photos est interdite. Si elle est requise, prière de communiquer avec le chargé de projet de l'organisation et la Section de la sécurité ministérielle de la GRC.

5. Il est interdit d'utiliser des biens personnels, p. ex. périphériques, dispositifs de communication ou dispositifs de stockage portatifs (clés USB), conjointement avec la technologie de la GRC.

6. L'entrepreneur n'a pas l'autorisation de divulguer des renseignements de nature délicate qui lui ont été fournis par la GRC à des sous-traitants qui n'ont pas la cote de sécurité de la GRC leur permettant de consulter les renseignements protégés.

7. La Section de la sécurité ministérielle de la GRC se réserve le droit :
   - d'inspecter les installations ou les locaux de l'entrepreneur. Des inspections peuvent être réalisées avant que des renseignements de nature délicate soient communiqués ou au besoin (p. ex. si le lieu de travail de l'entrepreneur change). L'inspection vise à s'assurer de la qualité des mesures de sécurité.
   - de demander une vérification des mesures de sécurité à l'aide de photos. Des photographies peuvent être demandées avant que des renseignements de nature délicate soient communiqués ou au besoin (p. ex. si le lieu de travail de l'entrepreneur change). La vérification à l'aide de photos vise à s'assurer de la qualité des mesures de sécurité.
   - de formuler des conseils sur les mesures de sécurité obligatoires (mesures de sécurité précisées dans le présent document et autres mesures possibles propres aux installations).

8. Afin d'assurer le contrôle souverain du Canada sur ses données, toutes les données délicates ou protégées qui sont sous le contrôle du gouvernement doivent être stockées sur des serveurs qui se trouvent au Canada. Les données en transit doivent être chiffrées adéquatement.

Sécurité matérielle

1. Aucun renseignement (documents papier, p. ex. notes) ou autre bien Protégé A ou B ne doit être retiré des installations de la GRC sans l'approbation du représentant de la GRC. Si cette approbation est obtenue, le transport, la transmission, le stockage et la destruction de ces renseignements ou autres biens doivent se faire conformément aux exigences de sécurité énoncées dans le *Manuel de la sécurité* de la GRC.

2. Seuls les dessins épurés doivent se trouver dans les installations de l'entrepreneur (c.-à-d. qu'ils ne contiennent pas de renseignements protégés ou classifiés). Afin d'épurer correctement les plans d'étage, l'entrepreneur doit s'assurer que les dessins satisfont aux exigences suivantes :

    - Les dessins de construction ne comportent pas de plan repère montrant l'ensemble du complexe ou des installations.
    - Les logos et le nom de la GRC ou l'adresse des installations ne figurent pas sur les dessins de construction.
    - Les identificateurs de Services publics et Approvisionnement Canada ou du gouvernement du Canada sont utilisés.
    - Les pièces sont identifiées par un numéro, et non par un nom. Une liste codée des numéros de pièces associés à l'information de nature délicate et aux descripteurs doit être conservée séparément et mise à jour à mesure que des changements sont apportés.
    - L'information sur le système de sécurité figure sur des couches différentes de dessin de construction pour faciliter l'impression et la distribution.

Sécurité des TI

1. Aucun renseignement de nature délicate, dont la classification de sécurité est Protégé A ou supérieure, ne doit être transmis par voie électronique à l'extérieur des réseaux de la GRC ou être traité à l'établissement de l'entrepreneur.

2. Aucun bien ou support électronique contenant des renseignements de nature délicate, dont la classification de sécurité est Protégé A ou supérieure, ne doit être retiré des réseaux ou des installations de la GRC.

3. Il est interdit d'utiliser des biens personnels, p. ex. périphériques, dispositifs de communication ou dispositifs de stockage portatifs (clés USB), conjointement avec la technologie de la GRC.

4. Il est interdit d'utiliser des appareils personnels pour se connecter à des réseaux de la GRC ou mener des activités sur ces réseaux de quelle que façon que ce soit dans les installations de la GRC, y compris créer un réseau ou un point d'accès.

5. Seuls les entrepreneurs qui ont la cote de fiabilité approfondie de la GRC peuvent utiliser un téléphone cellulaire personnel dans les locaux de la GRC (après en avoir obtenu l'autorisation); cependant :
    a. seuls des renseignements de nature non délicate peuvent être communiqués au moyen de cet appareil;
    b. cet appareil ne doit pas servir pour traiter des affaires de la GRC;
    c. cet appareil ne doit en aucun temps être connecté à des dispositifs de communication de la GRC.

6. Il est interdit de conserver des renseignements Protégé A et B, chiffrés ou non, dans des systèmes, des réseaux ou des supports de stockage, à moins d'être expressément autorisé à le faire.

Sécurité du personnel

1. Tous les employés de l'entrepreneur et des sous-traitants sont tenus d'obtenir et de conserver la cote de sécurité de la GRC correspondant au caractère délicat des travaux exécutés pendant toute la durée du contrat (conformément aux dispositions de la LVERS).

2. L'entrepreneur est chargé d'informer la GRC de tout changement concernant les exigences de sécurité relatives au personnel. Par exemple, si un employé possédant une cote de sécurité quitte l'entreprise ou n'est plus affecté au contrat conclu avec la GRC, lorsque de nouveaux employés doivent faire l'objet d'une vérification de sécurité et lorsque des employés doivent faire renouveler leur cote de sécurité.

Cote d'accès aux installations de niveau II : Lorsque l'entrepreneur et ses employés n'auront besoin d'avoir accès qu'aux installations ou aux sites de la GRC et n'auront pas accès à des renseignements, systèmes ou biens protégés ou classifiés, ils doivent obtenir une cote de sécurité de la GRC au niveau approprié. Les employés de l'entrepreneur doivent se soumettre à des vérifications effectuées par la GRC auprès du service de police local avant de pouvoir avoir accès aux installations. La GRC se réserve le droit d'interdire aux employés de l'entrepreneur d'accéder à ses sites ou installations, et ce, en tout temps.

Dans les cas où la GRC exige une **cote d'accès aux installations de niveau II**, l'entrepreneur doit lui faire parvenir les documents suivants :

- Formulaire SCT 330-23 (version VAC)
- Photocopie d'une pièce d'identité valide avec photo émise par le gouvernement (copie du permis de conduire recto verso)

La GRC :

- effectuera des vérifications de sécurité dont les exigences sont supérieures à celles énoncées dans la Politique sur la sécurité du gouvernement;
- est responsable de définir les exigences en matière d'escorte dans ses installations ou sur ses sites.

LISTE DE VÉRIFICATION DES EXIGENGES RELATIVES À LA SÉCURITÉ

PHASE II – SOLUTION FINALE

Government of Canada / Gouvernement du Canada

AMENDED SRCL# 202011119075 - FINAL SOLUTION

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité
PROTECTED A

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
RCMP	IM/IT - NHQ / CIO / SDPPM
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

The work to be performed includes design, architecture, configuration and implementation of the final National Cybercrime IM/IT Solution. An agile procurement process will be used. The work to be done will be performed by one of the (3) prototype vendors after issuance of the contract for the final solution. The final solution vendor will require access to RCMP facilities and may require access to ROSS and RCMP data.

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

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

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

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité PROTECTED A

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

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

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

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

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

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

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

Between prototype and the POP Test phase the FA2 resource will be subject to following restrictions until receiving the ERS(non-privileged access) o ERS+SECRET(privileged access):
- The FA2 resource cannot receive any RCMP login credentials;
- The FA2 resource must be escorted by an appropriately cleared individual; and
- The FA2 resource may guide an appropriately cleared individual who will have hands on keyboard.

Special comments:
Commentaires spéciaux :

For the Pop Test & Final Solution: Once the security levels are finalized and the list of resources to clear for the identified roles is received, the security clearance process will start during the POP test Phase.

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité
PROTECTED A

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

☐ No / Non ☑ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité
PROTECTED A

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Dusan Musal	Director, NC3 Project	Digitally signed by Musal,Dusan,000169308 Date: 2020.04.27 12:03:16 -04'00'	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613-998-7329		dusan.musal@rcmp-grc.gc.ca	2020/04/27

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sheila Nordskog	Security Analyst	SRCL AMENDED 2020-10-06 SNORDSKOG	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613-843-5247	613-823-0143	sheila.nordskog@rcmp-grc.gc.ca	2020-07-29

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

☐ No / Non ☑ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Mary Rutledge	A/Manager- Procurement Special Projects	Mary Rutledge	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
343-552-2386 / 613-843-6935		mary.rutledge@rcmp-grc.gc.ca	2020/05/15

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

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

Guide de sécurité – Liste de vérification des exigences relatives à la sécurité (LVERS)

Solution nationale en matière de cybercriminalité – Solution finale
LVERS n° 20201119075

Préparé par :
Section centrale de la sécurité ministérielle
Gendarmerie royale du Canada

Exigences générales de sécurité

Tous les entrepreneurs engagés dans le cadre du contrat visé par le présent guide sont tenus de collaborer au maintien de l'environnement de sécurité de la GRC en se conformant aux directives énoncées ci-après.

9. Tous les renseignements protégés (documents papier) et autres biens de nature délicate dont la GRC est responsable doivent être transmis à l'entrepreneur suivant des processus approuvés préalablement.

10. Les renseignements communiqués par la GRC doivent être gérés, tenus à jour et éliminés conformément aux clauses du contrat. À tout le moins, l'entrepreneur est tenu de respecter la *Politique sur la sécurité* du gouvernement.

11. L'entrepreneur doit aviser promptement la GRC de toute utilisation ou divulgation non autorisée de l'information communiquée en vertu du contrat visé par le présent guide et il doit transmettre à la GRC les détails de l'utilisation ou de la divulgation non autorisée (p. ex. en cas de perte, accidentelle ou délibérée, de renseignements de nature délicate).

12. La prise de photos est interdite. Si elle est requise, prière de communiquer avec le chargé de projet de l'organisation et la Section de la sécurité ministérielle de la GRC.

13. Il est interdit d'utiliser des biens personnels, p. ex. périphériques, dispositifs de communication ou dispositifs de stockage portatifs (clés USB), conjointement avec la technologie de la GRC.

14. L'entrepreneur n'a pas l'autorisation de divulguer des renseignements de nature délicate qui lui ont été fournis par la GRC à des sous-traitants qui n'ont pas la cote de sécurité de la GRC leur permettant de consulter les renseignements protégés.

15. La Section de la sécurité ministérielle de la GRC se réserve le droit :
    - d'inspecter les installations ou les locaux de l'entrepreneur. Des inspections peuvent être réalisées avant que des renseignements de nature délicate soient communiqués ou au besoin (p. ex. si le lieu de travail de l'entrepreneur change). L'inspection vise à s'assurer de la qualité des mesures de sécurité.
    - de demander une vérification des mesures de sécurité à l'aide de photos. Des photographies peuvent être demandées avant que des renseignements de nature délicate soient communiqués ou au besoin (p. ex. si le lieu de travail de l'entrepreneur change). La vérification à l'aide de photos vise à s'assurer de la qualité des mesures de sécurité.
    - de formuler des conseils sur les mesures de sécurité obligatoires (mesures de sécurité précisées dans le présent document et autres mesures possibles propres aux installations).

16. Afin d'assurer le contrôle souverain du Canada sur ses données, toutes les données délicates ou protégées qui sont sous le contrôle du gouvernement doivent être stockées sur des serveurs qui se trouvent au Canada. Les données en transit doivent être chiffrées adéquatement.

Sécurité matérielle

Les mesures de sécurité physique ci-dessous sont contingentes et subordonnées à l'autorisation appropriée accordée au sein de la liste de vérification des exigences de sécurité.

1. **Stockage :** Les renseignements et les biens protégés doivent être conservés dans un contenant approuvé par la Section de la sécurité ministérielle (SSM) de la GRC. Le contenant doit être situé (à tout le moins) dans une « zone de travail ». Ainsi, les installations de l'entrepreneur doivent comporter un secteur ou une pièce qui répond aux critères suivants :

Zone de travail	
Définition	Secteur dont l'accès est limité au personnel qui y travaille et aux visiteurs escortés comme il se doit. Nota : Le personnel qui travaille dans la zone de travail doit : • posséder une cote de fiabilité de la GRC valide ou • être escorté par une personne qui possède une cote de fiabilité de la GRC valide.
Périmètre	La zone de travail doit être délimitée par un périmètre reconnaissable ou un périmètre sécurisé selon les besoins du projet. Par exemple, les contrôles peuvent être un bureau ou un local verrouillé.
Surveillance	Surveillance périodique par des employés autorisés. Par exemple, les utilisateurs de l'espace de travail sont en mesure de déterminer s'il y a eu une infraction à la sécurité.

Nota : Consulter l'annexe A pour en savoir plus sur le concept de la zone de sécurité.

2. **Discussions :** Lorsque des conversations de nature délicate pourraient avoir lieu dans une zone de travail, celle-ci doit se trouver à une certaine distance des lieux publics ou être conçue selon des spécifications de protection acoustique (de façon à ce que l'utilisateur puisse raisonnablement présumer qu'il ne sera pas entendu). Par exemple : pièce/bureau privé ou salle de conférence.

3. **Production :** La production (génération ou modification) de renseignements ou biens protégés doit se faire dans un endroit qui répond aux critères d'une zone de travail.

4. **Destruction :** Toutes les ébauches et tous les documents mal imprimés ou imprimés par erreur (copies endommagées ou surplus) doivent être détruits par l'entrepreneur. Les renseignements protégés doivent être détruits conformément aux dispositions du *Manuel de la sécurité* de la GRC. L'équipement/les systèmes (p. ex. déchiqueteuse) utilisés pour détruire les documents de nature délicate sont cotés en fonction du degré de destruction. Il faut utiliser de l'équipement de destruction approuvé par la GRC.

   Niveaux approuvés pour la destruction de matériel Protégé B :

   - La dimension des lambeaux doit être inférieure à 1 x 14,3 mm (coupe en particules).

Nota :

- Si l'entrepreneur n'est pas en mesure de respecter les exigences de la GRC en matière de destruction, tous les renseignements et les biens de nature délicate doivent être retournés à la GRC aux fins de destruction.
- Toutes les ébauches et tous les documents de nature délicate mal imprimés ou imprimés par erreur en attente d'être éliminés doivent être protégés de la façon convenue jusqu'à leur destruction.

5. **Transport/transmission :** L'échange physique de renseignements de nature délicate doit se faire selon les normes du contrat. Si on a recours à un service de livraison, il doit fournir une preuve d'expédition, un suivi en transit et une preuve de livraison.

Transport	Transport : Transfert de renseignements et de biens de nature délicate d'une personne ou d'un endroit à un autre par une personne qui a besoin de connaître l'information ou d'accéder au bien.
Transmission	Transmission : Transfert de renseignements et de biens de nature délicate d'une personne ou d'un endroit à un autre par une personne qui n'a pas besoin de connaître l'information ou d'accéder au bien.

Nota :

- Pour le transport de renseignements Protégé B (déplacement vers/de lieux neutres aux fins de réunions et/ou d'entrevues) : Au lieu d'une simple enveloppe, on peut utiliser une serviette porte-documents ou tout autre contenant de solidité égale ou supérieure. Utiliser une double enveloppe/un emballage pour protéger le contenu fragile ou garder les paquets lourds ou volumineux intacts.
- Pour la transmission de renseignements Protégé B (Postes Canada ou courrier recommandé) : Adresser de manière non précise. Ajouter « À l'attention de » si le principe du besoin de connaître ou du besoin d'accès le justifie.

Sécurité des TI

Contrôle approprié de l'information désignée Protégé A et B

Transport et transmission

1. Les renseignements Protégé A ou B ne doivent pas être communiqués au public.

2. Il est interdit d'utiliser des biens personnels, p. ex. périphériques, dispositifs de communication ou dispositifs de stockage portatifs (clés USB), conjointement avec la technologie de la GRC.

3. Il est interdit à l'entrepreneur d'utiliser des appareils personnels pour se connecter à des réseaux de la GRC ou mener des activités sur ces réseaux de quelle que façon que ce soit dans les installations de la GRC, y compris créer un réseau ou un point d'accès.

4. L'entrepreneur peut transmettre de l'information Protégé A (communications vocales et données) au moyen de n'importe quel réseau sous la direction de la GRC et de l'infrastructure connexe approuvée par la GRC, sans avoir recours à des mesures de protection supplémentaires, par exemple le chiffrement.

5. L'entrepreneur peut traiter de l'information Protégé B localement sur des ordinateurs connectés au réseau ROSS, mais doit chiffrer cette information au moyen d'une solution de chiffrement standard pour la stocker ou la transmettre.

6. L'entrepreneur doit utiliser une solution de chiffrement approuvée par la GRC ou une application prévue pour le stockage de renseignements Protégé B pour transmettre de l'information Protégé B à l'intérieur de l'organisation (à l'aide de réseaux gérés par la GRC) et à l'extérieur de celle-ci.

Téléphonie

1. L'entrepreneur peut se servir des téléphones de bureau standard de la GRC pour communiquer des renseignements Protégé A.

   NOTA : Un téléphone de bureau s'entend d'un téléphone destiné à être branché au poste occupé par une personne par opposition à un téléphone mobile ou cellulaire.

2. Il est interdit d'utiliser les téléphones de bureau standard pour échanger de l'information Protégé B.

3. Seuls des renseignements de nature non délicate peuvent être communiqués à l'aide d'un appareil cellulaire ou mobile ou d'une ligne téléphonique terrestre, à moins que l'appareil soit spécifiquement homologué et fourni pour le traitement de données de nature délicate.

4. Seuls les entrepreneurs qui ont la cote de fiabilité approfondie de la GRC peuvent utiliser un téléphone cellulaire personnel dans les locaux de la GRC (après en avoir obtenu l'autorisation); cependant :
   - seuls des renseignements de nature non délicate peuvent être communiqués au moyen de cet appareil;

- cet appareil ne doit pas servir pour traiter des affaires de la GRC;
- cet appareil ne doit en aucun temps être connecté à des dispositifs de communication de la GRC.

Impression, numérisation par balayage et photocopie

1. Il est permis d'imprimer, de numériser ou de photocopier de l'information Protégé A ou B au moyen de l'équipement fourni par la GRC seulement.

Stockage

1. Il est interdit de conserver des renseignements Protégé A et B, chiffrés ou non, dans des systèmes, des réseaux ou des supports de stockage, à moins d'être expressément autorisé à le faire.

2. Lorsque les renseignements Protégé B ne sont pas utilisés, on doit les protéger :
    - en les chiffrant au moyen d'une solution de chiffrement approuvée par la GRC et en les conservant dans un système ROSS local ou un réseau ROSS;
    - à l'aide d'une application prévue pour le stockage de renseignements Protégé B;
    - au moyen de mesures de sécurité matérielle autorisées.

3. Les jetons ICP, les cartes d'identité, les cartes d'accès et tout autre objet utilisés pour ouvrir une session dans des applications, des systèmes et d'autres dispositifs technologiques, chiffrer ou déchiffrer des documents, apposer sa signature numérique sur des documents ou supprimer de l'information de façon sécurisée ne doivent jamais être laissés sans surveillance à proximité du dispositif technologique avec lequel ils sont utilisés.

4. Tous les dispositifs de stockage fournis par la GRC et utilisés pendant la durée du contrat doivent être retournés à la GRC immédiatement après la fin du contrat.

Sécurité du personnel

3. Tous les employés de l'entrepreneur et des sous-traitants sont tenus d'obtenir et de conserver la cote de sécurité de la GRC correspondant au caractère délicat des travaux exécutés pendant toute la durée du contrat (conformément aux dispositions de la LVERS).

4. L'entrepreneur est chargé d'informer la GRC de tout changement concernant les exigences de sécurité relatives au personnel. Par exemple, si un employé possédant une cote de sécurité quitte l'entreprise ou n'est plus affecté au contrat conclu avec la GRC, lorsque de nouveaux employés doivent faire l'objet d'une vérification de sécurité et lorsque des employés doivent faire renouveler leur cote de sécurité.

5. Comme l'entrepreneur et ses employés auront accès à des renseignements protégés ou classifiés de la GRC, ils devront obtenir une cote de sécurité de la GRC au niveau approprié. Les employés de l'entrepreneur doivent se soumettre à des vérifications effectuées par la GRC avant de pouvoir avoir accès aux systèmes, aux biens, aux installations ou aux renseignements protégés et/ou classifiés de la GRC. La GRC se réserve le droit d'interdire aux employés de l'entrepreneur d'accéder à ses systèmes, biens, installations et renseignements, et ce, en tout temps.

Dans les cas où la GRC juge nécessaire que les employés de l'entrepreneur détiennent une cote de fiabilité approfondie (CFA) ou une habilitation sécuritaire, l'entrepreneur doit lui faire parvenir les documents suivants :

1. Formulaire SCT 330-23 (version VAC)
2. Formulaire SCT 330-60
3. Formulaire 1020-1 de la GRC (questionnaire préalable à l'entrevue de sécurité/fiabilité)
4. Copie de l'acte de naissance et du permis de conduire de l'employé
5. Deux photos de taille passeport de l'employé

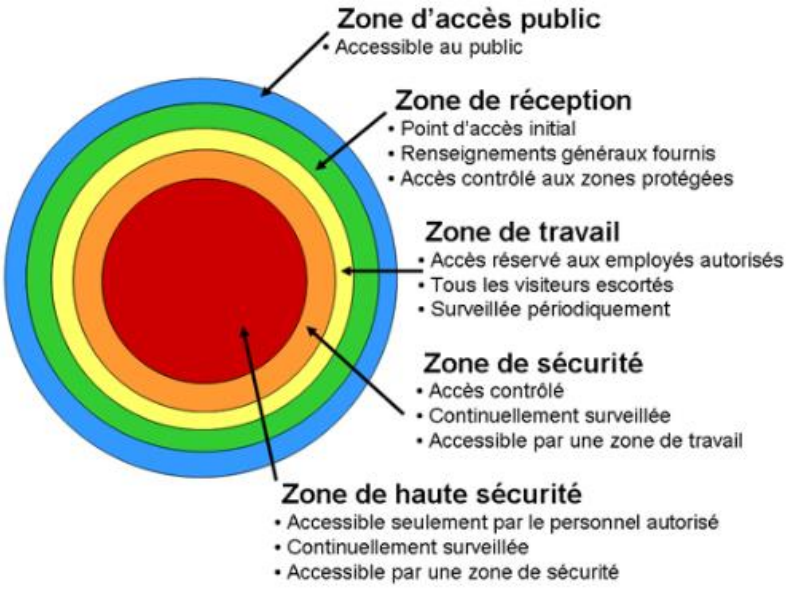
La GRC :

1. effectuera des vérifications de sécurité dont les exigences sont supérieures à celles énoncées dans la *Politique sur la sécurité* du gouvernement;
2. mènera une entrevue de sécurité;
3. s'occupera de la prise d'empreintes digitales.

Annexe A – Zones de sécurité

La *Politique sur la sécurité* du gouvernement (article 10.8 – Limites à l'accès) stipule que « les ministères doivent limiter l'accès aux renseignements classifiés et protégés et autres biens aux seules personnes qui ont besoin de les connaître et qui ont la cote de fiabilité ou de sécurité appropriée. »

Dans la *Norme opérationnelle sur la sécurité matérielle* (article 6.2 – Hiérarchie des zones), on précise que « les ministères doivent assurer l'accès et la protection des biens protégés et classifiés en fonction d'une hiérarchie des zones clairement reconnaissable. »



Zone d'accès public : zone où l'accès est libre pour le public et qui entoure habituellement un immeuble gouvernemental ou en fait partie. Exemples : les terrains entourant un immeuble et les corridors publics, ainsi que les vestibules d'ascenseur dans des immeubles à plusieurs occupants.

Zone d'accueil : espace où la transition d'une zone d'accès public à une zone à accès restreint est délimitée et contrôlée. Elle est située généralement à l'entrée de l'immeuble où survient le premier contact entre le public et le ministère, y compris des endroits où des services sont fournis et où des renseignements sont échangés. L'accès au public peut être restreint pendant certaines heures de la journée ou pour des motifs particuliers.

Zone de travail : zone dont l'accès est limité au personnel qui y travaille et aux visiteurs escortés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée sur une base périodique. Par exemple, des bureaux à aire ouverte ou un local électrique typiques.

Zone de sécurité : zone dont l'accès est limité au personnel autorisé et aux visiteurs autorisés et escortés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée continuellement (24 heures sur 24, 7 jours sur 7). Par exemple, une zone où des renseignements secrets sont traités ou conservés.

Zone de haute sécurité : zone dont l'accès est limité au personnel autorisé qui détient une cote de sécurité valide et de niveau approprié et aux visiteurs autorisés et escortés comme il se doit; elle doit être indiquée au moyen d'un périmètre bâti selon les caractéristiques techniques recommandées dans l'évaluation de la menace et des risques, surveillée continuellement (24 heures sur 24, 7 jours sur 7) et être un secteur où les détails de l'accès sont enregistrés et vérifiés. Par exemple, une zone où des biens de grande valeur sont manipulés par des employés sélectionnés.

L’accès à ces zones devrait être fondé sur le principe du « besoin de connaître » et être restreint afin de protéger les employés et les biens de valeur. Pour de plus amples renseignements, il est recommandé de consulter le document G1-026 Guide pour l’établissement des zones de sécurité matérielle de la GRC.

APPENDICE A À L'ANNEXE C –

GUIDE DE CLASSIFICATION DE LA SÉCURITÉ

Le tableau suivant présente les exigences en matière d'attestation de sécurité du personnel et des installations en fonction des rôles prévus et de l'accès aux données du GC.

Tableau A-1 Guide de classification de sécurité pour les services infonuagiques commerciaux

Nº	Rôle ou fonction	Prévision concernant le type de données consulté	Accès aux données Lieu (Canada ou l'étranger ou les deux)	Filtrage nécessaire	Responsabilité	Détails
1.	Tout membre du personnel de l'entrepreneur ayant un accès physique aux centres de données de l'entrepreneur	• Matériel physique • Installations de centres de données • Données telles qu'elles sont stockées sur des supports de sauvegarde locaux de l'entrepreneur	Canada	Fiabilité	Entrepreneur	Cela concerne le personnel de l'entrepreneur, notamment les ressources chargées de la gestion des installations qui ont physiquement accès au matériel lié aux services infonuagiques dans les centres de données de l'entrepreneur.
2.	Tout membre du personnel de l'entrepreneur ayant un accès logique aux services de l'entrepreneur	• Toutes les données opérationnelles • Données telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur	Les deux	Fiabilité	Entrepreneur	Cela concerne le personnel de l'entrepreneur qui a un accès logique aux données du GC hébergées dans les centres de données de l'entrepreneur et à tout système sensible de même qu'aux données sur les incidents de sécurité.

Nº	Rôle ou fonction	Prévision concernant le type de données consulté	Accès aux données Lieu (Canada ou l'étranger ou les deux)	Filtrage nécessaire	Responsabilité	Détails
3.	Tout membre du personnel de l'entrepreneur qui a des rôles privilégiés et un accès logique non restreint à des biens du GC dans les services de l'entrepreneur	• Toutes les données opérationnelles • Données du GC telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur • Biens dont les données et les justificatifs du GC	Les deux	Secret	Entrepreneur	Cela concerne le personnel de l'entrepreneur qui a des privilèges élevés assortis d'un accès logique sans restriction aux données du GC hébergées dans les centres de données de l'entrepreneur et à tout système sensible de même qu'aux données sur les incidents de sécurité. Cela comprend l'accès autorisé par l'intermédiaire d'un processus établi comme les demandes juridiques.
4.	Tout membre du personnel ou revendeur de l'entrepreneur qui a accès à l'information du compte maître du et/ou aux justificatifs du GC	• Information du compte maître ou justificatifs du GC	Les deux	Fiabilité	Entrepreneur et/ou revendeur	Cela concerne tout membre du personnel de l'entrepreneur ou d'un revendeur qui a accès au compte maître du GC ou aux justificatifs racines pour la configuration des comptes des services infonuagiques.
5.	Entrepreneur principal*	Supports	Les deux	Fiabilité	Entrepreneur	Information qui est envoyée de l'entrepreneur principal au sous-traitant – doit être chiffrée.
6.	Directeur des opérations / personnel*	Noms, adresses, courriels, numéros de téléphone et centres de données	Les deux	Fiabilité	Entrepreneur	Information qui est envoyée de l'entrepreneur principal au sous-traitant – doit être chiffrée.
7.	Tâches générales	Zones publiques et de d'accueil	Les deux	S.O.	Entrepreneur	

Nº	Rôle ou fonction	Prévision concernant le type de données consulté	Accès aux données Lieu (Canada ou l'étranger ou les deux)	Filtrage nécessaire	Responsabilité	Détails
8.	Tâches générales*	Sites sensibles (comme les zones opérationnelles où les données sont stockées)	Les deux	Cote de fiabilité	Entrepreneur	*L'information sur place peut être de nature sensible. Les personnes qui n'ont pas été filtrées doivent être escortées en tout temps. Les tâches générales comprennent la prestation de services d'entretien, la présence de gardiens de sécurité dans la zone opérationnelle, etc.

*L'entrepreneur doit communiquer avec la DSIC de SPAC pour s'assurer que la LVERS secondaire appropriée est établie pour les sous-traitants.

APPENDICE B À L'ANNEXE C –

OBLIGATIONS EN MATIÈRE DE SÉCURITÉ

Obligations en matière de sécurité

Les obligations de l'entrepreneur contenues dans les présentes obligations de sécurité doivent être transférées par le fournisseur aux sous-processeurs du fournisseur, dans la mesure où elles s'appliquent à chaque sous-processeur du fournisseur, compte tenu de la nature des services infonuagiques publics fournis à l'entrepreneur.

1. Gestion du changement.

a) Le fournisseur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir à jour les obligations en matière de sécurité afin de se conformer aux pratiques de sécurité des normes de l'industrie.

b) L'entrepreneur doit aviser le Canada de toutes les améliorations qui pourraient avoir une incidence sur les services dans le contrat, y compris les améliorations techniques, administratives ou tout autre type d'améliorations. L'entrepreneur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans supplément pour le Canada.

2. Reconnaissance.

Les parties reconnaissent que :

a) Tous les biens et les actifs informationnels sont assujettis à ces obligations en matière de sécurité.

b) Nonobstant toute autre disposition du contrat, les parties partagent la responsabilité d'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux biens et aux actifs informationnels.

3. Transfert et récupération des données.

À la demande du Canada, l'entrepreneur doit :

a) extraite tous les actifs d'information en ligne, pseudo-directs et hors ligne, y compris, sans toutefois s'y limiter, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités infonuagiques, les codes source hébergés dans un référentiel de codes du Canada et les configurations réseau, de sorte que le client puisse se servir de ces instructions pour effectuer la migration d'un environnement à un autre;

b) effectuer le transfert sécurisé de tous les actifs d'information, y compris les métadonnées, dans un format lisible et utilisable par machine acceptable pour le Canada, conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue de Bibliothèque et Archives Canada (https://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formats-fichier-transferers-ressources-documentaires.aspx).

4. Disposition des dossiers et remise des dossiers au Canada.

a) L'entrepreneur doit, à la demande du Canada, éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent des actifs d'information et s'assurer que les données précédemment stockées ne peuvent être traitées par d'autres clients après leur diffusion. Cela touche toutes les copies des actifs d'information du Canada qui sont créées à des fins de disponibilité accrue et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être harmonisée à l'un des documents suivants : (i) Manuel d'utilisation du Programme

national de sécurité industrielle (DoD 5220.22-M6); (ii) Lignes directrices pour l'assainissement des supports (NIST SP 800-88); ou (iii) Effacement et déclassification des supports d'information électroniques (CSTC ITSG-06).

b) L'entrepreneur doit, à la demande du Canada, fournir des preuves démontrant qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirés ou détruits après leur retrait de l'instance du Canada.

5. Surveillance continue.

a) L'entrepreneur doit continuellement gérer, surveiller et maintenir la posture de sécurité de tous les biens, de l'infrastructure du fournisseur et des emplacements de service pendant toute la durée du contrat, et s'assurer que les services fournis au Canada sont conformes aux présentes obligations en matière de sécurité. Dans le cadre de l'obligation, l'entrepreneur doit :

(i) surveiller activement et continuellement les menaces et les vulnérabilités pesant sur les actifs, l'infrastructure de l'entrepreneur, les emplacements de service ou les actifs d'information;

(ii) faire de son mieux pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le refus de service;

(iii) faire de son mieux pour détecter les attaques, les incidents de sécurité et autres événements anormaux;

(iv) détecter l'utilisation et l'accès non autorisés à tous les services infonuagiques publiques, données et composants pertinents aux services IaaS, PaaS ou SaaS du Canada;

(v) gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de remédier à tout problème signalé publiquement dans les services infonuagiques publics ou les bibliothèques que la solution utilise, et fournir des avis préalables liés aux correctifs conformément aux engagements convenus relatifs au niveau de service;

(vi) répondre aux menaces et aux attaques contre les services du fournisseur, les contenir et veiller à la récupération;

(vii) au besoin, prendre des contre-mesures proactives, y compris, des mesures préventives et d'intervention permettant d'atténuer les menaces.

b) Les services infonuagiques publics de l'entrepreneur doivent permettre de copier les données des applications (IaaS, PaaS et SaaS) et le trafic réseau (IaaS et PaaS) du gouvernement du Canada dans les services infonuagiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).

c) Les services infonuagiques publics de l'entrepreneur doivent permettre au Canada de déployer et d'utiliser des logiciels de sécurité pour assurer la surveillance avancée et l'atténuation des cybermenaces pour la solution du Canada à l'échelle de l'hôte géré par le gouvernement et de la couche réseau, pour les composants gérés par le Canada seulement.

6. Notifications.

a) L'entrepreneur doit fournir :

(i) une notification rapide de toute interruption qui peut avoir une incidence sur la disponibilité et le rendement du service (comme convenu entre les parties et indiqué dans l'énoncé de travail ou l'entente sur les niveaux de service [ENS]);

(ii) des bilans réguliers au sujet des procédures de restauration des services à un état opérationnel selon les ENS et les exigences en matière de disponibilité du système convenues, sous forme d'alertes transmises avant et après la mise en œuvre;

(iii) des alertes, des avis et des directives de sécurité liés au système d'information, par courriel, pour les vulnérabilités qui constituent une menace pour la solution.

7. Intervention en cas d'incident de sécurité

a) Si l'entrepreneur prend connaissance d'une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès accidentel ou illégal aux données du client ou des données personnelles du client pendant le traitement par l'entrepreneur (chacun étant un « incident de sécurité »), l'entrepreneur doit rapidement et sans tarder (i) informer le Canada de cet incident de sécurité; (ii) mener une enquête et fournir des renseignements détaillés sur cet incident de sécurité; (iii) prendre les mesures raisonnables pour atténuer les effets et les dommages découlant de l'incident de sécurité.

b) L'entrepreneur doit alerter et aviser promptement le Canada (par téléphone et par courriel) de toute compromission, de toute violation ou de toute preuve comme (i) un incident de sécurité, (ii) une défectuosité liée à la sécurité d'un actif, (iii) l'accès irrégulier ou non autorisé à un actif, (iv) la copie à grande échelle d'un actif d'information ou (v) toute autre activité illégale recensée par l'entrepreneur, portant ce dernier à croire de manière raisonnable que le risque de compromission, d'atteinte à la sécurité ou à la vie privée est ou pourrait être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année), et sans tarder, dans tous les cas, dans les 24 heures.

c) L'entrepreneur doit collaborer avec le Canada au confinement, à l'éradication et à la récupération des incidents de sécurité conformément au processus d'intervention en cas d'incident de sécurité de l'entrepreneur et au Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) (https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html). Notamment :

(i) ne permettre qu'aux représentants désignés du Canada :

i. de demander et de recevoir des renseignements liés à l'incident de sécurité et à tout actif d'information compromis (y compris, données des utilisateurs, journaux d'événements du système et de sécurité, saisies de paquets du réseau ou de l'hôte, journaux de composants de sécurité comme des systèmes de détection et de prévention d'intrusion et des pare-feux, etc.), dans un format non chiffré, à des fins de réalisation d'enquêtes;

ii. d'assurer le suivi de l'état d'un événement signalé lié à la sécurité de l'information ou d'un incident de sécurité.

(ii) de soutenir les efforts d'enquête du Canada en cas de compromission relevée des utilisateurs ou des données de la solution.

d) L'entrepreneur doit :

(i) tenir un registre des violations de la sécurité comprenant une description de la violation de la sécurité, la durée, les conséquences de la violation, le nom de la personne ayant

signalé la violation, et la personne à qui la violation a été signalée, et la procédure pour récupérer les données ou le service;

(ii) assurer le suivi ou permettre au Canada d'assurer le suivi des divulgations d'actifs et de renseignements, y compris les données qui ont été divulguées, à qui, et à quel moment.

8. Preuve électronique et mises en suspens pour raisons juridiques

L'entrepreneur doit (et doit, dans la mesure où cela s'applique compte tenu de la nature des services infonuagiques données en sous-traitance fournis par chaque sous-traitant de l'entrepreneur, exiger des sous-traitants qu'ils prennent des mesures raisonnables pour) s'assurer que la solution offre des fonctions de communication de la preuve électronique et de mises en suspens pour raisons juridiques pour les journaux des événements de sécurité afin de permettre au Canada de mener rapidement et efficacement des enquêtes de sécurité et de répondre aux demandes des tribunaux en matière de mises en suspens pour raisons juridiques.

9. Mise à l'essai de l'évaluation de sécurité

L'entrepreneur doit disposer d'un processus qui permet au Canada d'effectuer une analyse de vulnérabilité ou un essai de pénétration non perturbateur et non destructif visant la partie canadienne des composantes de la solution dans l'environnement de l'entrepreneur.

10. Sous-traitants

a) L'entrepreneur doit fournir une liste de sous-traitants auxquels il pourrait faire appel pour exécuter n'importe quelle partie des travaux en fournissant la solution au Canada. La liste doit comprendre les renseignements suivants : (i) le nom du sous-traitant; (ii) la description des services infonuagiques publics qui seraient offerts par le sous-traitant; et (iii) les emplacements où le sous-traitant offrirait les services infonuagiques publics.

b) L'entrepreneur doit fournir une liste des sous-traitants dans les dix jours suivant la date d'entrée en vigueur du contrat. L'entrepreneur doit aviser le Canada (en mettant à jour le site Web et en fournissant au client un mécanisme lui permettant d'obtenir un avis lié à cette mise à jour) au sujet de tout nouveau sous-traitant au moins 14 jours avant de fournir aux sous-traitants l'accès aux données du client ou aux données personnelles. L'entrepreneur doit aider le Canada à mener les vérifications visant les sous-traitants dans les dix jours ouvrables.

11. Gestion des risques de la chaîne d'approvisionnement

Dans les 30 jours suivant l'attribution du contrat, l'entrepreneur doit fournir un plan de gestion des risques de la chaîne d'approvisionnement (PGRCA) mis à jour, évalué et validé de manière indépendante par un tiers indépendant certifié selon le régime de certification de l'AICPA ou de CPA Canada ou de l'ISO. Le plan PGRCA doit être fourni au Canada sur une base annuelle, ou sur demande, ou immédiatement après tout changement important du plan PGRCA.

APPENDICE C À L'ANNEXE C –

AUTRES RENSEIGNEMENT SUR LA SÉCURITÉ À L'INTENTION DES ENTREPRENEURS ET DES SOUS-TRAITANTS ÉTRANGERS

L'**entrepreneur ou le sous-traitant** étranger destinataire doit mener une enquête de sécurité auprès de tous les membres de son personnel qui devront avoir accès à des renseignements de niveau **PROTÉGÉ AU CANADA** :

a) Vérification de l'identité
   i. Copies de deux pièces d'identité originales valides émises par le gouvernement, dont une avec photo
   ii. Nom de famille
   iii. Prénoms complets (souligner ou encercler le prénom usuel)
   iv. Nom de famille à la naissance
   v. Tous les autres noms utilisés (surnoms)
   vi. Changement de nom
      1. En cas de changement de nom, fournir l'ancien nom et le nouveau nom, le lieu du changement et l'institution ayant officialisé le changement.
   vii. Sexe
   viii. Date de naissance
   ix. Lieu de naissance (ville, province ou État et pays)
   x. Citoyenneté(s)
   xi. État civil/union de fait
      1. Situation actuelle (marié, conjoint de fait, séparé, veuf, divorcé, célibataire)
      2. Renseignements sur tous les époux actuels (s'il y a lieu)
         a. Nom de famille
         b. Prénoms complets (souligner ou encercler le prénom usuel)
         c. Date et durée du mariage ou de l'union de fait
         d. Date de naissance
         e. Nom de famille à la naissance
         f. Lieu de naissance (ville, province ou État et pays)
         g. Citoyenneté

b) Vérification de résidence
   i. Historique de résidence des cinq (5) dernières années, en commençant par l'adresse la plus récente, sans intervalle
      1. Numéro d'appartement, numéro de rue, nom de la rue, ville, province ou État, code postal, pays, dates d'arrivée et de départ
c) Vérification des études
   i. Établissements d'enseignement fréquentés et dates correspondantes
d) Vérification des antécédents professionnels
   i. Historique des emplois des cinq (5) dernières années, en commençant par l'emploi le plus récent, sans intervalle
   ii. Trois (3) références d'emploi durant les cinq (5) dernières années
e) Vérification de casier judiciaire
   i. Rapport(s) contenant toutes les condamnations criminelles des cinq (5) dernières années à l'intérieur ou à l'extérieur du pays de résidence du candidat.

ANNEXE D

DEFINITIONS ET INTERPRETATIONS

Dans le présent contrat, à moins que le contexte n'exige une interprétation différente, les termes suivants doivent avoir le sens prévu ci-dessous :

- « **ACAC** » ou « **contrôle d'accès basé sur les attributs** » désigne une méthode de contrôle d'accès logique dans laquelle l'autorisation d'effectuer un ensemble d'opérations est déterminée en évaluant les attributs associés au sujet, à l'objet, aux opérations demandées et, dans certains cas, aux conditions d'environnement par rapport à la politique, aux règles ou aux relations qui décrivent les opérations autorisées pour un ensemble donné d'attributs (nist.gov).
- **« Utilisateur actif »** désigne un utilisateur enregistré qui dispose d'un compte d'utilisateur et de références pour accéder à la Solution.
- « **AD** » ou « **Active Directory** » signifie un service de répertoire développé par Microsoft pour les réseaux qui appartiennent au domaine Windows pour gérer les ordinateurs et les autres périphériques sur un réseau (microsoft.com)[1].
- L'« **analyse avancée** » désigne l'examen autonome ou semi-autonome des données ou du contenu à l'aide de techniques et d'outils de pointe, habituellement au-delà de ceux liés aux renseignements d'entreprise traditionnels afin d'accroître la compréhension, de faire des prévisions ou de formuler des recommandations. Les techniques d'analyse avancée comprennent notamment l'exploration de données et de texte, l'apprentissage automatique, le filtrage, les prévisions, la visualisation, l'analyse sémantique, l'analyse des sentiments, l'analyse de réseau et l'analyse par grappes, les statistiques à variables multiples, l'analyse de graphiques, la simulation, le traitement d'événements complexes et les réseaux neuronaux (Gartner.com).
- « **Recherche avancée** » signifie une recherche dans une base de données à l'aide de méthodes comme la proximité, les caractères de remplacement, la troncature, l'appariement par phrase ou mot-clé ou l'utilisation d'opérateurs booléens pour restreindre (« et ») ou élargir (« ou ») la recherche de renseignements stockés.
- **« IA »** ou **« Intelligence artificielle »** signifie l'application de techniques d'analyse avancée et de techniques fondées sur la logique, y compris l'apprentissage automatique pour interpréter les événements, appuyer et automatiser les décisions, et prendre des mesures (Gartner.com).
- « **EIA** » ou « **Évaluation de l'incidence algorithmique** » désigne un questionnaire destiné à aider les concepteurs à évaluer et atténuer les risques associés au déploiement d'un système de décision automatisé. L'EIA fournit aux concepteurs une mesure pour évaluer les solutions d'IA d'un point de vue éthique et humain, afin qu'elles soient conçues de manière responsable et transparente (Canada.ca)[2].
- « **API** » ou « **Interface de programmation d'applications** » désigne une interface qui permet aux développeurs d'interagir avec les programmes et les applications, y compris les systèmes de gestion de l'apprentissage.
- « **Appli** » signifie Application.
- « **Actif** » signifie toutes les ressources en matière de technologies de l'information auxquelles l'entrepreneur a accès ou les ressources de cette nature qu'il utilise ou gère pour assurer la prestation et la livraison des services décrits dans la présente entente (y compris, *non exclusivement*, toutes les ressources technologiques se trouvant aux emplacements de service de l'entrepreneur, ou encore, dans un centre de données, un réseau, un dispositif de stockage, des serveurs, des plateformes de

---

1 https://fr.wikipedia.org/wiki/Active_Directory

2 https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/evaluation-incidence-algorithmique.html

virtualisation, des systèmes d'exploitation, des intergiciels et des applications de l'entrepreneur *ou d'un sous-traitant de celui-ci*).

- « **PEA** » ou « **plan d'essai d'acceptation** » désigne le processus d'essai d'acceptation, comme les caractéristiques à tester, les critères de réussite ou d'échec, l'approche à la mise à l'essai, les listes de contrôle, les rôles et responsabilités, les exigences en matière de ressources et les calendriers. Le PEA définit également la fonctionnalité à mettre à l'essai, les exigences vérifiées par l'essai, les conditions préalables à l'essai, les étapes de l'essai et les conditions postérieures à l'essai. Les testeurs de logiciels déterminent si le logiciel répond aux exigences du client, c'est-à-dire si ce dernier est prêt à accepter le logiciel dans son environnement (klariti.com)[3].
- « **REA** » ou « **rapport d'essai d'acceptation** » désigne un rapport, principalement adressé aux développeurs de logiciels, qui résume les essais effectués et leurs résultats. Le REA devrait tenter de classifier la gravité de chaque non-conformité ou échec de l'essai et doit définir chaque essai de façon unique (ing.iac.es)[4].
- « **Utilisateur autorisé** » désigne tout utilisateur qui détient un profil d'accès à la solution valide avec un accès défini par un profil de RBAC ou ACAC.
- **« Accès utilisateur Autorisé »** désigne le droit accordé au Canada par l'entrepreneur d'utiliser la solution et ses services connexes, tels que définis dans l'énoncé des travaux pour un modèle de distribution de type logiciel en tant que service (SaaS) ou hybride.
- « **MCO** » ou « **Modèle de capacité opérationnelle** » désigne un document qui représente les points de vue de haut niveau d'une organisation du point de vue de ses capacités opérationnelles et qui décrit brièvement ce qu'une organisation fait. Il s'agit généralement d'un ensemble de capacités opérationnelles de haut niveau à l'échelle de l'organisation.
- « **RE** » ou « **renseignements d'entreprise** » désigne les applications, l'infrastructure et les outils, ainsi que les pratiques exemplaires permettant l'accès à l'information et l'analyse de l'information pour améliorer et optimiser les décisions et le rendement (Gartner.com).
- **« Traitement des mégadonnées »** désigne des techniques permettant d'analyser et d'extraire systématiquement des renseignements utiles à partir d'ensembles de données à grande échelle.
- « **BOLO** » ou « **Be On the Lookout** » s'entend d'une émission qui contient des attributs permettant d'identifier un suspect, une personne ou un autre objet d'intérêt pour l'application de la loi et qui est diffusée à des partenaires de l'application de la loi ou au sein d'un organisme d'application de la loi dans le but de résoudre un crime ou d'obtenir des renseignements criminels.
- **« Recherche booléenne** » utilise des connecteurs pour combiner des termes de recherche. Il existe trois connecteurs : ET, OU et PAS.
    - **ET** : Placé entre les mots, ce qui signifie que les deux mots doivent apparaître dans chaque référence. Ceci limitera la recherche, par exemple : la recherche renaissance ET musique récupérera toutes les références qui contiennent les deux termes.
    - **OU** : Placé entre les mots, ce qui signifie que l'un ou l'autre ou tous les mots peuvent apparaître dans chaque référence. Ceci élargira la recherche, par exemple : tremblement de terre OU séismologie récupérera toutes les références avec tremblement de terre ou séismologie, ainsi que les références avec les deux termes.
    - **PAS** : Placé entre les mots, ce qui signifie que le deuxième mot ne doit apparaître dans aucune référence. Ceci limitera la recherche, par exemple : la recherche toxique PAS radioactive récupérera toutes les références avec toxique, sauf celles qui incluent radioactif.
- « **Canada** », « **Couronne** », « **Sa Majesté** » ou « **l'État** » désignent Sa Majesté la reine du chef du Canada, représentée par le ministre de Travaux publics et Services gouvernementaux et toute autre personne dûment autorisée à agir au nom de ce ministre.

---

3 https://klariti.com/2018/09/24/what-is-an-acceptance-test-plan

4 http://www.ing.iac.es/~eng/standards/software/sof-std-4/node19.html

- « **Données du Canada** » désigne les renseignements ou les données, peu importe la forme ou le format de ceux-ci : A) divulgués par le personnel, les clients, les partenaires, les participants à une coentreprise, les concédants de licence, les vendeurs ou les entrepreneurs du Canada, ou liés à ceux-ci; B) divulgué par les utilisateurs finaux des services ou en rapport avec eux; ou C) recueillis, utilisés ou traités par les services ou entreposés pour ceux-ci; qui sont divulgués directement ou indirectement à l'entrepreneur ou aux sous-traitants de l'entrepreneur par le Canada ou les utilisateurs finaux ou en leur nom.
- « **CAD** » signifie dollar canadien.
- « **CAFC** » ou « **Centre antifraude du Canada** » désigne l'organisme central au Canada qui recueille de l'information et des renseignements criminels sur des questions comme la fraude par marketing de masse (par exemple, le télémarketing), la fraude des frais payables à l'avance (par exemple, la fraude par lettre en Afrique de l'Ouest), la fraude par Internet et les plaintes pour vol d'identité.
- « **RAC** » signifie Rapport sur les activités cybercriminelles.
- « **Gestion des cas** » désigne un processus complexe qui exige une combinaison de tâches humaines et de processus électronique, comme une demande reçue, une réclamation soumise, une plainte ou une réclamation qui fait l'objet d'un litige. Ce processus peut comprendre des processus, la collaboration en matière de gestion, le stockage d'images et de contenu, la prise de décisions et le traitement de dossiers ou de cas électroniques (Gartner.com).
- « **CCC** » ou « **Centre canadien pour la cybersécurité** » est un organisme gouvernemental qui aide à renforcer la résilience et la sécurité du Canada en matière de cybersécurité par l'entremise de ses conseils, de ses conseils, de son expertise et de ses partenariats. Le CCC offre un guichet unique de conseils et de services d'experts aux gouvernements, aux exploitants d'infrastructures essentielles et au secteur public et privé pour renforcer leur cybersécurité (www.cyber.gc.ca/fr).
- « **CCSJ** » ou « **Centre canadien de la statistique juridique** » désigne le centre au sein de Statistique Canada qui est le centre de coordination de la collecte fédérale-provinciale-territoriale de renseignements sur la nature et l'étendue de la criminalité et l'administration de la justice pénale au Canada (securitepublique.gc.ca)[5].
- « **CEF** » ou « **Common event format** » signifie un format standard de l'industrie, en plus des messages du journal d'exploitation, utilisé par de nombreux fournisseurs de sécurité pour permettre l'interopérabilité des événements entre différentes plateformes.
- « **Certification** » désigne l'action ou le processus consistant à fournir à une personne ou à une organisation un document officiel attestant de l'état ou du niveau de réalisation. Certaines certifications sont obligatoires et représentent une condition à l'emploi.
- « **IC/LC** » ou « **processus d'intégration continue et livraison continue** » désigne une pratique exemplaire de méthodologie agile qui permet aux équipes de développement de logiciels de se concentrer sur la satisfaction des besoins opérationnels et la qualité du code et la sécurité, étant donné que les étapes de déploiement sont automatisées. CICD incarne une culture, un ensemble de principes d'exploitation et une collection de pratiques qui permettent aux équipes de développement d'applications d'apporter des changements de code de manière plus fréquente et fiable (infoworld.com)[6].
- « **Client** » désigne le ministère ou l'organisme pour lequel le travail ou les services sont exécutés aux termes du contrat. À cet égard, le client peut faire référence à tout ministère, organisme et société d'État du gouvernement ou à toute autre entité de la Couronne visée par la *Loi sur la gestion des finances publiques* (tpsgc-pwgsc.gc.ca)[7].

---

5 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/msrng-cnd/index-fr.aspx

6 https://www.infoworld.com/article/3271126/what-is-cicd-continuous-integration-and-continuous-delivery-explained.html

7 https://www.tpsgc-pwgsc.gc.ca/comm/index-fra.html

- « **Services infonuagiques** » désigne un style de calcul dans lequel les capacités évolutives et élastiques d'utilisation de l'informatique sont fournies en tant que service utilisant les technologies Internet (Gartner.com).
- **« MPSI » ou « modèle de prestation de service d'infonuagique »** désigne la manière dont les services d'infonuagique sont fournis au consommateur. Trois modèles fondamentaux sont définis : infrastructure (IaaS), plateforme (PaaS) et logiciel (SaaS). Un MPSI peut être constitué d'un seul ou d'une combinaison de tous les modèles, appelée MPSI « hybride ».
- « **Dossier de plainte** » désigne le site Web de signalement public sur lequel seront recueillis les rapports sur la cybercriminalité et la fraude provenant du public ou des petites et moyennes entreprises. Les dossiers de plainte sont automatiquement incorporés dans la solution de SNCC au moyen d'une interface avec le site Web de signalement public.
- « **Recherche conceptuelle** » s'entend d'une recherche basée sur un ou plusieurs concepts précisés par l'utilisateur qui décrit les documents à renvoyer comme les résultats de la recherche. Il peut s'agir d'une technique utile de définition des documents possiblement pertinents lorsqu'un ensemble de mot-clés n'est pas connu à l'avance.
- « **Utilisateurs simultanés** » le nombre total d'utilisateurs autorisés qui utilisent la solution en même temps (par exemple, pour l'exécution des requêtes, la saisie de données, la visualisation et la production de rapports).
- « **Conteneurisation** » désigne l'encapsulation ou le regroupement du code logiciel et de toutes ses dépendances, de sorte qu'il puisse fonctionner de manière uniforme et constante sur toute infrastructure. La conteneurisation permet aux développeurs de créer et déployer des applications de manière rapide et en toute sécurité. La conteneurisation permet aux applications d'être écrites une fois et exécutées n'importe où (ibm.com/ca-fr).
- « **Contrat** » s'entend des articles du contrat, de toute condition générale, de toute condition générale supplémentaire, de toutes les annexes et de tout autre document qui sont inscrits au contrat, dans leur version ponctuellement modifiée avec l'accord des parties.
- « **Autorité contractante** » signifie la personne désignée comme telle dans le contrat, ou dans un avis à l'entrepreneur, pour représenter le Canada dans l'administration du contrat.
- « **Entrepreneur** » désigne l'entité nommée dans le contrat pour fournir les services ou les travaux au Canada.
- « **Corrélation** » ou « **corréler** » désigne une relation entre deux ou plusieurs éléments d'information.
- « **Coût** » désigne le coût établi conformément aux Principes des coûts contractuels 1031-2 en vigueur à la date de la demande de soumissions ou, s'il n'y a pas eu de demande de soumissions, à la date du contrat.
- « **COTS** » ou « **disponible sur le marché** » désigne les logiciels et le matériel informatique qui existent déjà et qui sont disponibles à partir de sources commerciales. On les appelle aussi « de série » (nist.gov).
- « **GP** » signifie gestionnaire de projet. Il s'agit d'une personne au sein de l'organisation de l'entrepreneur responsable de la bonne exécution du contrat.
- « **UCT** » désigne l'unité centrale de traitement, qui est le circuit électronique d'un ordinateur exécutant les instructions qui constituent un programme informatique. L'UCT effectue des opérations arithmétiques et logiques et des opérations de contrôle et d'entrée ou de sortie de base précisées par les instructions du programme.
- « **GRC** » signifie la gestion des relations avec la clientèle.
- « **CRTC** » ou « **Conseil de la radiodiffusion et des télécommunications canadiennes** » désigne un tribunal administratif sans lien de dépendance avec le gouvernement fédéral. Le CRTC s'engage à s'assurer que les Canadiens ont accès à un système de communication de classe mondiale qui encourage l'innovation et enrichit leur vie. Le rôle du CRTC est d'appliquer les lois et les règlements établis par les parlementaires qui créent la législation et les ministères qui établissent les politiques. Le

Conseil réglemente et surveille les secteurs canadiens de la radiodiffusion et des télécommunications dans l'intérêt public (crtc.gc.ca)[8].

- « **CST** » signifie Centre de la sécurité des télécommunications. Il s'agit de l'organisme national de cryptologie du gouvernement du Canada. Administré par le ministère de la Défense nationale, il est responsable des renseignements électromagnétiques étrangers et de la protection des réseaux électroniques d'information et de communication du gouvernement du Canada.
- **« FSI »** ou **fournisseur de services infonuagiques** désigne l'entité qui possède, exploite et entretient l'infrastructure (« nuage ») et fournit des ressources informatiques virtualisées aux consommateurs. Le FSI peut fournir une infrastructure informatique de base telle que le calcul et le stockage des données ou des solutions complètes sous forme de logiciels hébergés.
- « **ECC** » signifie évaluation des capacités et de la convivialité. L'ECC est utilisée pour analyser la capacité d'une organisation de développement à exécuter une conception axée sur l'utilisateur.
- « **Cyber** » désigne Internet et les technologies de l'information comme les ordinateurs, les tablettes ou les appareils mobiles.
- « **Cybercrime** » désigne tout crime dans lequel la cybernétique – Internet et les technologies de l'information comme les ordinateurs, les tablettes ou les appareils mobiles – joue un rôle déterminant dans la perpétration d'une infraction criminelle. La GRC divise la cybercriminalité en deux catégories : la technologie comme cible, où le crime ne peut être commis qu'en utilisant des ordinateurs, des réseaux et des appareils numériques, et la technologie comme instrument, où Internet et les technologies de l'information jouent un rôle déterminant dans le crime (rcmp-grc.gc.ca).
- « **Taxonomie de la cybercriminalité** » désigne la taxonomie qui fournit un langage uniforme dans tous les organismes d'application de la loi nord-américains dans le but d'accroître la production de rapports, la documentation et la communication de renseignements, ainsi que dans le but d'améliorer la législation et de permettre une analyse statistique comparable.
- « **Cybersécurité** » désigne une combinaison de personnes, de politiques, de processus et de technologies qui sont utilisés par une entreprise pour protéger ses biens cybernétiques (Gartner.com).
- « **Gardien des données** » désigne une personne ou organisation qui détient ou contrôle des données informatiques. Elle est pertinente au traitement d'une demande ou d'un ordre de préservation.
- « **Demande de conservation de données** » désigne une demande faite par un agent de la paix ou d'un fonctionnaire en vertu de l'article 487 012 du Code criminel du Canada, qui exige la préservation de données informatiques précises par la personne qui les possède ou les contrôle. Les demandes de préservation de données émises au nom d'une administration étrangère expirent 90 jours après leur délivrance au gardien des données. Les demandes de préservation de données émises par un organisme canadien chargé du contrôle d'application de la loi expirent 21 jours après leur délivrance au gardien des données. Les demandes de conservation de données peuvent être émises une fois pour les renseignements, ce qui signifie qu'une demande de préservation ne peut pas être renouvelée.
- « **Ordre de préservation de données** » s'entend d'une ordonnance rendue par un agent de la paix ou un fonctionnaire public en vertu de l'article 487 013 du Code criminel du Canada qui exige la préservation de données informatiques par les personnes qui les possèdent ou qui les contrôlent. Avant la publication, un ordre de préservation de données doit d'abord être assermenté devant un juge de paix ou un juge. Les ordres de préservation de données expirent 90 jours après leur délivrance au gardien des données. Ces ordres peuvent être renouvelés.
- « **Demande de préservation de données** » s'entend d'une demande visant à préserver les données qui sont transmises au Canada depuis une administration étrangère ou qui sont transmises du Canada vers une administration étrangère. Les demandes de préservation de données et les ordres subséquents de cette nature sont créés et gérés par le point de contact de l'UNCLC, ouvert 24 heures sur 27, 7 jours sur 7, en fonction des demandes de préservation de données et des demandes de prolongation reçues d'administrations étrangères.

8 https://crtc.gc.ca/fra/accueil-home.htm

- « **SGBD** » signifie système de gestion de base de données.
- « **Harmoniser** » désigne l'ajustement ou la coordination pour prévenir ou résoudre un conflit (par exemple, si plusieurs services de police s'intéressent à un serveur de réseau, l'harmonisation implique la détermination et l'atténuation de leurs intérêts mutuels).
- « **Produit livrable** » ou « **produits livrables** » signifie, dans un sens générique, toute partie distincte du travail à accomplir pour le Canada.
- « **Appareil** » désigne tout équipement muni d'une unité centrale de traitement (UCT), d'une mémoire de grande capacité, d'appareils d'entrée et de sortie (par exemple, un clavier, une souris, un microphone et un écran) et de serveurs, d'ordinateurs de bureau, d'ordinateurs portatifs, d'assistants numériques personnels et d'équipement informatique mobile.
- « **DevOps** » est un ensemble de pratiques qui combine le développement de logiciels (Dev) et les opérations de technologie de l'information (Ops) et vise à raccourcir le cycle de développement des systèmes et fournir une prestation continue avec une qualité logicielle élevée.
- « **DHCP** » désigne le protocole de configuration dynamique des hôtes, qui est un protocole de gestion du réseau utilisé sur les réseaux à protocole Internet, par lequel un serveur DHCP attribue de manière dynamique une adresse IP et d'autres paramètres de configuration du réseau à chaque appareil sur un réseau afin de lui permettre de communiquer avec d'autres réseaux IP. Un serveur DHCP permet aux ordinateurs de demander automatiquement des adresses IP et des paramètres réseau au fournisseur d'accès Internet (FAI), ce qui réduit la nécessité pour un administrateur réseau ou un utilisateur d'affecter manuellement des adresses IP à tous les appareils de réseau.
- « **Date d'agenda** » désigne une date et un horodatage de système appliqués aux notes et aux notes de service.
- « **Documents à communiquer** » désigne la capacité de cerner, d'évaluer et de sélectionner les documents d'un dossier ou d'un projet, y compris les dossiers, les formulaires, les déclarations, les rapports, les données et les activités, dans le but de préparer des documents à communiquer aux fins de présentation à des services de police partenaires ou au tribunal.
- « **PRC** » désigne un plan de reprise après catastrophe.
- « **DNS** » signifie système de noms de domaine, un système de noms hiérarchisé et décentralisé pour les ordinateurs, les services ou d'autres ressources qui sont connectés à Internet ou à un réseau privé.
- « **Accéder en mode descendant** » signifie accéder à des données qui se trouvent dans un niveau inférieur d'une base de données structurée de façon hiérarchique.
- « **SDSM** » désigne la Direction générale de la sécurité ministérielle de la GRC.
- « **Norme Dublin pour les métadonnées** » est un petit ensemble de termes de vocabulaire prédéfinis qui peuvent être utilisés pour décrire des ressources Web (vidéo, images, pages Web, etc.), ainsi que des ressources physiques comme des livres ou des CD, et des objets comme des œuvres d'art. Ils offrent des renseignements de catalogage élargis et une indexation améliorée des documents pour les programmes de moteurs de recherche.
- « **PCSM** » désigne le profil de contrôle de sécurité ministérielle de la GRC.
- « **CE3** » ou « **Centre européen de lutte contre la cybercriminalité** » désigne l'organe d'Europol qui coordonne les activités transfrontalières d'application de la loi contre la criminalité informatique et qui agit en tant que centre d'expertise technique en la matière. Le CE3 a été créé en 2013 pour renforcer la réponse des forces de l'ordre à la cybercriminalité dans l'UE et aider à protéger les citoyens, les entreprises et les gouvernements européens. Chaque année, le CE3 publie l'Évaluation de la menace du crime organisé sur Internet, son rapport stratégique phare sur les principales conclusions et les nouvelles menaces et nouveaux développements dans le domaine de la cybercriminalité (europol.europa.eu)[9].

[9] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- « Utilisateur final » désigne un utilisateur ayant accès à la solution nationale en matière de cybercriminalité.
- « **Enrichissement** » signifie ajouter de la valeur par corrélation, agrégation, recherche, analyse et collecte des résultats.
- « **Entité** » signifie tout objet d'une base de données sur lequel nous voulons modéliser et stocker des renseignements. Les entités sont souvent des concepts reconnaissables, concrets ou abstraits, comme une personne, des endroits, des éléments ou des événements qui sont pertinents dans le cadre de la base de données. Les personnes, les véhicules, les lieux, les organisations, les numéros de téléphone et les pièces justificatives, entre autres, sont des exemples précis d'entités qui ont des données à leur sujet.
- « **Erreur** » désigne toute instruction ou instruction contenue *ou non contenue* dans la solution qui, par sa présence ou son absence, l'empêche de fonctionner conformément aux spécifications.
- « **ETC** » signifie extrait, transformation et chargement, qui est la procédure générale de reproduire des données d'une ou de plusieurs sources dans un système de destination qui représente les données différemment de la ou des sources ou qui les représente dans un contexte différent de celui de la ou des sources.
- « **ESRI** » désigne l'Environmental Systems Research Institute, qui est un fournisseur de solutions de systèmes d'information géographique d'entreprise.
- « **Europol** » désigne l'organisme chargé de l'application des lois de l'Union européenne (UE), créé en 1998 pour traiter les renseignements criminels et lutter contre la criminalité internationale organisée et grave et le terrorisme, par la coopération entre les autorités compétentes des États membres de l'UE (europol.europa.eu)[10].
- « **Codes de traitement d'Europol** » s'entend des codes de traitement définis par Europol pour transmettre les souhaits du fournisseur en matière de partage et de sécurité des renseignements. Les codes de traitement sont les suivants :
  - T1 – Les renseignements ne doivent pas être utilisés comme éléments de preuve dans les procédures judiciaires sans l'autorisation du fournisseur.
  - T2 – Les renseignements ne doivent pas être diffusés sans l'autorisation du fournisseur.
  - T3 – D'autres restrictions s'appliquent et doivent être incluses comme instructions texte.
- « **Recherche de syntagme exacte** » signifie la recherche d'une chaîne de mots comme expression exacte. Les références ne seront récupérées que si les mots se trouvent côte à côte (par exemple, la technologie de l'information). Dans certaines bases de données, la recherche exige que le syntagme soit placé entre guillemets (par exemple, « technologie de l'information »).
- « **Document d'exploitation** » désigne un document susceptible d'offenser un adulte raisonnable qui décrit ou dépeint une personne ou la représentation d'une personne qui est, ou est en apparence, un enfant de moins de 16 ans :
  - dans un contexte sexuel, y compris, par exemple, dans le cadre d'une activité sexuelle;
  - dans un contexte choquant ou dégradant;
  - en train d'être soumis à des actes de maltraitance, de cruauté ou de torture.
- **«Utilisateur externe»** signifie un utilisateur autorisé du Portail des partenaires et des policiers (P3)
- « **FBI** » signifie Federal Bureau of Investigation, le service national de renseignement et de sécurité des États-Unis et son principal organisme fédéral d'application de la loi.
- « **FBI IC3** » s'entend de l'Internet Crime Complaint Centre du FBI, dont la mission est de fournir au public un mécanisme de signalement fiable et commode pour la transmission de renseignements au Federal Bureau of Investigation sur les activités criminelles présumées facilitées par Internet, en plus de permettre l'élaboration d'alliances efficaces avec les organismes d'application de la loi et les partenaires de

10 https://www.europol.europa.eu/fr/about-europol

l'industrie. Les renseignements sont analysés et diffusés à des fins d'enquête et de renseignement aux forces de l'ordre et à des fins de sensibilisation du public[11].

- « **Dossier** » désigne un concept de billet qui a été évalué et jugé approprié (qui répond aux exigences de mandat, de gravité et de priorité) pour être traité par l'UNCLC. Les dossiers peuvent contenir de nombreux billets ou être liés les uns aux autres.
- « **CANAFE** » ou « **Centre d'analyse des opérations et déclarations financières du Canada** » désigne l'unité du renseignement financier du Canada. Son mandat consiste à faciliter la détection, la prévention et la dissuasion en matière de blanchiment d'argent et de financement des activités terroristes, tout en protégeant les renseignements personnels sous son contrôle.
- **« COF »** ou **« Capacité opérationnelle finale »** signifie que les capacités décrites dans le MCO sont entièrement fournies et utilisées par l'unité du GNCC et d'autres parties prenantes pour mener des activités commerciales.
- « **Recherche en texte intégral** » désigne les techniques de recherche dans un document unique ou dans une collection, à l'intérieur d'une base de données de texte intégral ou de documents, selon des critères définis par l'utilisateur. Dans le cadre d'une recherche en texte intégral, le moteur de recherche examine tous les mots de chaque document stocké en essayant de les faire correspondre aux critères de recherche.
- « **Recherche floue** » désigne un processus qui localise des renseignements susceptibles d'être pertinents pour un critère de recherche, même s'ils ne correspondent pas exactement au résultat de la recherche. Les correspondances exactes ou très pertinentes apparaissent en haut de la liste. Des cotes de pertinence subjective, habituellement sous forme de pourcentages, peuvent être attribuées.
- « **Go** » signifie gigaoctet, qui est une unité informatique composée de 1 024 mégaoctets.
- « **GC** » ou « **GdC** » désigne le gouvernement du Canada.
- Les « **Normes numériques du GC** » ou « **Normes numériques du gouvernement du Canada** » sont le fondement de la transition du gouvernement du Canada vers une souplesse, une ouverture et une facilité d'utilisation accrues. Elles guident les équipes dans la conception de services numériques, d'une façon qui sert le mieux les Canadiens (Canada.ca).
- « **GIU** » signifie interface graphique, qui est une forme d'interface utilisateur qui permet aux utilisateurs d'interagir avec des appareils électroniques à l'aide d'icônes graphiques et d'indicateurs audio, comme la notation primaire, au lieu d'interfaces utilisateur par texte, d'étiquettes de commandes dactylographiées ou de navigation par texte.
- « **SIG** » signifie système d'information géographique.
- « **HOST** » est le principal symposium qui facilite la croissance rapide de la recherche et du développement sur la sécurité qui sont fondés sur le matériel. Depuis 2008, HOST est l'événement mondialement reconnu pour les chercheurs et les praticiens qui souhaitent faire avancer les connaissances et les technologies liées à la sécurité et à l'assurance du matériel.
- « **AC** » désigne l'administration centrale.
- « **HTML** » signifie le langage de balisage hypertexte qui est le langage de balisage standard des documents conçus pour être affichés sur un navigateur Web.
- « **IaaS** » ou « **Infrastructure comme service** » signifie une méthode de prestation de service d'infonuagique par laquelle un fournisseur de services infonuagiques fournit au consommateur des ressources informatiques de base telles que des serveurs, le traitement, le stockage et la mise en réseau qui permettent au consommateur de déployer et d'exécuter des logiciels arbitraires, y compris des systèmes d'exploitation et des applications. Le consommateur ne gère pas ou ne contrôle pas l'infrastructure en nuage sous-jacente, mais maîtrise des systèmes d'exploitation, le stockage et des applications mises en place, et maîtrise peut-être partiellement certaines composantes de réseautage (par exemple les pare-feu hôtes).

11 https://www.ic3.gov/

- « **Infrastructure IaaS** » signifie l'infrastructure gérée par le consommateur et fournie en tant que service (par exemple, centre de données, réseautage, stockage, serveurs, plateforme de virtualisation) et comprend les systèmes, le matériel et les logiciels utilisés pour gérer, exploiter et provisionner une infrastructure IaaS.
- « **IBM** » signifie International Business Machines Corporation.
- **« SDI ou SPI** » désigne un système de détection d'intrusion ou un système de prévention d'intrusion. Il s'agit d'un appareil ou d'une application logicielle qui surveille un réseau ou des systèmes pour détecter toute activité malveillante ou violation à la politique.
- « **GCVI** » signifie gestion du cycle de vie des informations.
- « **GI ou TI** » signifie la gestion de l'information ou la technologie de l'information.
- « **Ressources d'information** » désigne tout élément de données individuel de ces données canadiennes.
- « **Fuite de renseignements** » désigne des incidents où une ressource d'information est déposée par inadvertance dans un dispositif ou dans un système qui n'est pas autorisé à traiter ces renseignements (par exemple, LDSTI-33, IR-9).
- « **Capacité opérationnelle initiale** » signifie une solution opérationnelle provisoire qui est mise en œuvre pour permettre à l'UNCLC de mener ses opérations jusqu'à ce que la solution mise au point par la présente demande de proposition (DP) soit en place.
- « **INTELEX** » désigne un programme national de demande d'information géré par la GRC. Les demandes d'information INTELEX sont distribuées à différentes unités régionales ou divisionnaires INTELEX où les systèmes locaux sont interrogés. Les résultats sont recueillis et retournés au demandeur.
- « Utilisateur interne » ou « utilisateur principaux » désigne un utilisateur de la SNC qui accède à la Solution directement – et non pas par l'entremise du Portail des partenaires et des policiers. Les utilisateurs internes consisteront principalement en des ressources de la GRC, comme les employés du GNCC et la GI-TI, la Division nationale ou les ressources des Opérations techniques.
- « **Interopérabilité** » désigne la mesure dans laquelle les éléments de matériel et de logiciel peuvent fonctionner ensemble.
- « **IDC** » ou « **Indicateurs de compromission** » signifie une preuve médico-légale qui indique (avec une grande confiance) une intrusion informatique. Les IDC typiques sont les signatures de virus, les adresses IP, les algorithmes de hachage MD5 de fichiers de logiciels malveillants, les URL ou les noms de domaine des serveurs de contrôle et de commandement de réseau de zombies.
- « **IP** » désigne le protocole Internet qui est la méthode ou le protocole par lequel les données sont envoyées d'un ordinateur à un autre sur Internet. Chaque ordinateur (connu sous le nom d'ordinateur hôte) sur Internet possède au moins une adresse IP qui le distingue de tous les autres ordinateurs sur Internet.
- **« ISO »** signifie Organisation internationale de normalisation.
- « **FAI** » signifie le fournisseur d'accès Internet qui est un organisme de prestation de services d'accès à Internet ou d'utilisation d'Internet. Les fournisseurs de services Internet peuvent être organisés sous diverses formes, comme une entreprise à des fins commerciales, communautaires, à but non lucratif ou privé, ou bien une organisation détenue par des intérêts privés.
- « **TI** » signifie technologie de l'information.
- « **PCTI** » signifie plan de continuité de la technologie de l'information.
- « **Sécurité de TI** » ou « **Sécurité des technologies de l'information** » désigne un ensemble de stratégies de cybersécurité qui empêchent l'accès non autorisé aux ressources organisationnelles comme les ordinateurs, les réseaux et les données (Cisco.com).
- « **CSTI** » signifie Conseils en matière de sécurité des technologies de l'information.
- « **ITSP** » désigne le Guide de sécurité des technologies de l'information à l'intention du praticien.

- « **J-CAT** » ou « **Groupe d'action mixte en matière de cybercriminalité (J-CAT)** » est composé d'une équipe permanente d'agents de liaison sur la cybercriminalité des États membres de l'Union européenne (UE) et de pays partenaires non membres de l'UE. Il existe 13 organismes d'application de la loi issus de 11 pays qui ont accès aux bases de données d'Europol sur le renseignement en matière de cybercriminalité. J-CAT travaille sur la cybercriminalité avec un lien avec le Canada, y compris les logiciels malveillants, les réseaux de zombies et les intrusions, le blanchiment d'argent en ligne, la cryptomonnaie et la cyberfraude. Hébergé par le Centre européen de lutte contre la cybercriminalité (CE3), le groupe a pour mission de mener une action coordonnée et dirigée par les services de renseignement contre les principales menaces de cybercriminalité par des enquêtes et des opérations transfrontalières menées par ses partenaires.
- « **JPEG** » ou « **Groupe mixte d'experts en photographie** » est une méthode de compression avec perte couramment utilisée pour les images numériques, en particulier pour celles produites par photographie numérique. Le niveau de compression peut être ajusté pour permettre un choix de compromis entre la taille du stockage et la qualité de l'image.
- « **JSON** » signifie JavaScript Object Notation, un format de données indépendant du langage qui utilise du texte lisible par les humains pour stocker et transmettre des objets de données composés de paires d'attributs ou de valeurs et un éventail de types de données [12].
- « **Ko** » signifie kilo-octet, qui est une unité multiple utilisée pour les données binaires. Bien que le terme « kilo » désigne généralement 1 000 octets en informatique, un kilo-octet fait souvent référence à 1 024 octets. Cette mesure est souvent utilisée pour décrire la capacité de mémoire et le stockage sur disque.
- « **Recherche par mot-clé** » signifie la recherche à l'aide de mots-clés utilisés pour identifier le contenu des documents. L'utilisation par mot-clé peut faciliter la recherche et en améliorer la fiabilité.
- « **AL** » signifie application de la loi, c'est-à-dire tout système par lequel certains membres du gouvernement agissent de manière organisée pour faire respecter la loi en découvrant, en dissuadant, en réhabilitant ou en punissant les personnes qui violent les règles et normes qui régissent la société en question.
- « **NACCP** » s'entend des normes de l'Association canadienne des chefs de police. L'Association canadienne des chefs de police (ACCP) a créé NACCP en tant que comité opérationnel chargé d'assurer l'interopérabilité de l'échange de données sur la base du NIEM.
- « **Mise à niveau de maintenance** » désigne l'ensemble disponible sur le marché des améliorations, des extensions, des mises à niveau, des mises à jour, des versions, des renommages, des réécritures, des améliorations croisées, des composants et des mises à niveau inférieur ou toute autre modification apportée à la solution développée ou publiée par l'entrepreneur ou son ayant droit.
- « **Logiciel malveillant** » désigne un logiciel qui est intentionnellement inclus ou inséré dans un système à des fins malveillantes sans l'autorisation du propriétaire. Les formes courantes de logiciels malveillants comprennent les virus, les vers, les chevaux de Troie, les logiciels espions, les épouvantiels, les appeleurs automatiques, les programmes malveillants furtifs, les trousses d'exploitation et les rançongiciels.
- « **Échantillon de logiciels malveillants** » désigne un code malveillant qui n'a pas été modifié par les efforts des programmes de recherche automatique de virus et de programmes malveillants, ce qui fournit ainsi aux organismes de services d'application de la loi et d'analyse de programmes malveillants des échantillons intacts pour analyse et hachage.
- « **Service d'analyse des logiciels malveillants** » signifie un service fourni par une organisation externe qui, au minimum, gère une bibliothèque de valeurs de hachage de logiciels malveillants. En outre, le service pourrait effectuer une analyse d'un échantillon de logiciels malveillants et fournir un rapport

[12] https://fr.wikipedia.org/wiki/JavaScript_Object_Notation

détaillant les résultats de cette analyse. Les organisations de services d'analyse des logiciels malveillants comprennent le CCC, le FBI et l'EMAS.

- « **Gérer** » signifie, dans le contexte d'un système d'information, des actions comme la création, la modification, la suppression et l'accès à l'information ou aux documents.
- « **Message** » désigne une communication du système ou de l'utilisateur qui contient des informations, des actions ou des réponses.
- « **CO** » signifie critères obligatoires.
- « **Métadonnées** » signifie des données qui fournissent des renseignements sur d'autres données.
- « **APF** » signifie authentification par plusieurs facteurs, qui est une méthode d'authentification par laquelle un utilisateur d'ordinateur n'obtient l'accès qu'après avoir réussi à présenter deux ou plusieurs éléments de preuve à un mécanisme d'authentification.
- « **MISP** » ou « **Malware Information Sharing Platform** » désigne une plateforme libre et ouverte de communication des menaces qui facilite le partage de renseignements sur les menaces, y compris les indicateurs de cybersécurité. MISP est une plateforme de renseignement sur les menaces qui permet de recueillir, de partager, de stocker et de corréler les indicateurs de compromis des attaques ciblées, des renseignements sur les menaces, des renseignements sur la fraude financière, des renseignements sur la vulnérabilité, ou même des renseignements sur la lutte contre le terrorisme.
- « **AA** » ou « **apprentissage automatique** » désigne un sous-ensemble de l'intelligence artificielle qui utilise des modèles statistiques servant à extraire des connaissances et des tendances à partir de données afin de résoudre des problèmes.
- Le « **TEJ** » ou « **Traité d'entraide judiciaire** » est un accord international entre des États (gouvernements) sous forme écrite, régi par le droit international. Les TEJ sont un moyen par lequel des pays comme le Canada reçoivent des éléments de preuve aux fins d'utilisation dans le cadre d'enquêtes criminelles et de poursuites pénales ou aident à les recueillir. TEJ est un accord conclu entre deux ou plusieurs pays dans le but de recueillir et d'échanger des renseignements dans le but de faire respecter le droit public et pénal. Les États modernes ont mis au point des mécanismes permettant de demander et d'obtenir des éléments de preuve en vue d'enquêtes criminelles et de poursuites pénales.
- **« PMV »** ou **« produit minimum viable »** désigne un prototype de solution qui répond au minimum aux exigences des cinq (5) scénarios d'ECC de l'appendice A jusqu'à l'annexe A - Énoncé des travaux.
- « **UNCLC** » ou « **Unité nationale de coordination de la lutte contre la cybercriminalité** » désigne une unité composée à la fois d'agents de la GRC et de civils de divers milieux. L'UNCLC collaborera avec les organismes d'application de la loi et d'autres partenaires afin de réduire la menace que représente la cybercriminalité au Canada, ses répercussions et sa victimisation au Canada (rcmp-grc.gc.ca).
- Le « **CNCEE** » ou « **Centre national de coordination contre l'exploitation des enfants** » sert de point de contact pour les enquêtes sur l'exploitation sexuelle des enfants sur Internet au Canada. Le CNCEE est le principal portail du Canada pour toutes les questions liées à l'exploitation sexuelle des enfants sur Internet, y compris celles qui s'adressent aux organismes internationaux et celles qui proviennent d'organismes étrangers et destinées au Canada. Le CNCEE valide les demandes internationales et prépare et diffuse des dossiers d'enquête à la bonne administration du Canada.
- « **SNSICF** » ou « **Système national de signalement des incidents de cybercriminalité et de fraude** » désigne le site Web de signalement public en cours d'élaboration dans le cadre de l'ensemble du SNC. Le SNSICF sera utilisé par le public canadien et les petites et moyennes entreprises pour signaler les cybercrimes et les fraudes.
- « **NCFTA** » ou « **National Cyber-Forensics & Training Alliance** » est une société à but non lucratif fondée en 2002, dont l'objectif est d'identifier, d'atténuer et de neutraliser les menaces de cybercriminalité dans le monde. La NCFTA fonctionne en procédant à des échanges de renseignements et à des analyses en temps réel avec des experts en la matière (EM) dans les secteurs public, privé et universitaire. Grâce à ces partenariats, la NCFTA détecte de manière proactive les cybermenaces afin d'aider les partenaires à prendre des mesures préventives pour atténuer ces menaces.
- « **SNC** » désigne la solution nationale de cybercriminalité.

- « **EP de la SNC** » s'entend de l'environnement de production de la SNC.
- « **EE de la SNC** » désigne l'environnement d'essai de la SNC.
- Le « **NIEM** » ou « **National Information Exchange Model** » est un vocabulaire commun qui permet l'échange de renseignements entre divers organismes publics et privés. Le NIEM met en relation des communautés de personnes qui partagent un besoin commun d'échanger des renseignements afin de faire avancer leur mission. Le modèle est considéré comme un dictionnaire de termes, de définitions, de relations et de formats convenus qui sont indépendants de la façon dont l'information est stockée dans des systèmes individuels.
- « **TLN** » ou « **traitement du langage naturel** » s'entend de la technologie qui consiste à transformer le texte ou la parole audio en information codée et structurée, fondée sur une ontologie appropriée.
- « **Notification** » désigne un courriel adressé à un utilisateur ou à un groupe qui indique qu'un message ou une tâche lui a été envoyé ou mis à sa disposition.
- « **OAuth** » fournit aux clients un « accès délégué sécurisé » aux ressources de serveur pour le compte d'un propriétaire de ressources. Il précise un processus permettant aux propriétaires de ressources d'autoriser l'accès extérieur à leurs ressources de serveur sans partager leurs justificatifs d'identification.
- « **Observable** » Voir indicateurs de compromis.
- « **ROC** » ou « **Reconnaissance optique de caractères** » désigne un processus ou un composant qui extrait du texte à partir d'images de lettres imprimées ou manuscrites.
- « **Autres ministères** » s'entend de ministères et d'organismes fédéraux autres que la GRC.
- La **« *Loi sur les langues officielles*** » est une loi canadienne entrée en vigueur le 9 septembre 1969 qui accorde au français et à l'anglais un statut égal au sein du gouvernement du Canada.
- « **Source ouverte** » désigne un logiciel qui est fourni avec l'autorisation de l'utiliser, de le reproduire et de le distribuer, en l'état ou avec des modifications, et qui peut être offert gratuitement ou moyennant un frais. Le code de source doit être accessible (Gartner.com).
- « **OpenID** » désigne une norme ouverte et un protocole d'authentification décentralisé. Il permet aux utilisateurs d'être authentifiés par des sites coopérants à l'aide d'un service tiers, ce qui élimine la nécessité pour les administrateurs de site de fournir leurs propres systèmes de connexion ad hoc et permet aux utilisateurs de se connecter à plusieurs sites Web indépendants sans devoir posséder une identité et un mot de passe séparés pour chacun.
- « **SE** » désigne un système d'exploitation qui est un logiciel de base qui gère le matériel informatique et les ressources logicielles et qui fournit des services communs pour les programmes informatiques.
- Les « **RSO** » ou « **renseignements de source ouverte** » sont des données recueillies auprès de sources accessibles au public dont l'utilisation est prévue dans un contexte de renseignement. Dans la communauté du renseignement, le terme « ouvert » fait référence à des sources ouvertes et accessibles au public (par opposition à des sources secrètes ou clandestines). Il n'est pas lié aux logiciels ouverts ou aux renseignements publics.
- « **P3** » ou « **Portail des partenaires et des policiers** » désigne le portail externe qui offre un moyen de communication sécuritaire entre l'UNCLC et la police canadienne et les partenaires autorisés de la lutte contre la cybercriminalité. L'accès au P3 est strictement contrôlé par RBAC. Le P3 permet des demandes de renseignements externes visant les données stockées dans le dépôt de la SNC ainsi que la soumission de données, de cas et de demandes de services sur la cybercriminalité. Le P3 est également utilisé par l'UNCLC pour rendre les rapports publics sur la cybercriminalité accessibles aux services de police compétents et échanger des renseignements avec la police et les partenaires.
- « Utilisateur du P3 » désigne un utilisateur autorisé à utiliser le Portail des partenaires et des policiers de la SNC.
- **« PaaS »** ou **« plateforme en tant que service »** est une méthode de prestation de service d'infonuagique par laquelle un fournisseur de services infonuagiques (FSI) fournit une plateforme sur laquelle le consommateur peut construire, fournir et soutenir des applications et des services sur Internet. Les

serveurs, le système d'exploitation et autres services tels que la base de données, l'intergiciel sont gérés par le FSI.

- **« PaaS privée »** signifie qu'une PaaS est téléchargée et hébergée sur l'espace infonuagique de la GRC.
- **« PaaS publique »** signifie qu'une PaaS est hébergée par un fournisseur de services infonuagiques (FSI).
- « **PB** » signifie Protégé B.
- « **PDF** » désigne le format de document portable, un format de fichier dans lequel tous les éléments d'un document imprimé ont été saisis sous la forme d'une image électronique qu'il est possible de consulter, d'imprimer ou de transférer à une autre personne.
- Les « **renseignements personnels** » font référence aux renseignements qui concernent une personne identifiable et qui sont enregistrés sous quelque forme que ce soit, au sens de l'article 3 de la *Loi sur la protection des renseignements personn*els. Voici une liste non exhaustive de renseignements relatifs à la race, à la nationalité, à l'origine ethnique, à la religion, à l'âge, à l'état civil, à l'adresse, à l'éducation ainsi qu'aux antécédents médicaux, criminels, financiers ou aux antécédents d'emploi d'une personne. Les renseignements personnels comprennent également tout numéro ou symbole d'identification, comme le numéro d'assurance sociale, attribué à une personne. Définition tirée du site Web de la législation maintenu par le gouvernement du Canada : https://laws-lois.justice.gc.ca/fra/lois/P-21/section-3.html.
- « **EFVP** » s'entend de l'Évaluation des facteurs relatifs à la vie privée, qui est un type d'évaluation des répercussions effectuée par une organisation. Il s'agit normalement d'un organisme ou d'une société d'État qui a accès à une grande quantité de données confidentielles et privées sur des personnes qui se trouvent dans son système ou qui y transitent. L'évaluation aide les organisations à cerner et à gérer les risques liés à la protection de la vie privée découlant de nouveaux projets, initiatives, systèmes, processus, stratégies, politiques et relations d'affaires.
- « **Liste déroulante** » signifie une liste de choix (affichée sous forme de liste) pouvant être affichée sur une interface utilisateur, à partir de laquelle un seul élément peut normalement être sélectionné.
- **« ICP** » signifie infrastructure à clés publiques. Son objectif est de faciliter le transfert électronique sécuritaire de renseignements pour un éventail d'activités de réseau, comme le commerce électronique, les services bancaires par Internet et le courrier électronique confidentiel. Elle est requise pour les activités où les mots de passe simples sont une méthode d'authentification inadéquate.
- « **PNG** » ou « **Portable Network Graphics** » est un format de fichier d'infographie par quadrillage qui supporte la compression de données sans perte. Le format PNG a été développé comme un substitut amélioré et non breveté pour le format d'échange graphique (GIF).
- Le « **BP** » ou « bureau de projet » est parfois appelé bureau de gestion de projet. Son rôle consiste à offrir un soutien et des renseignements sur la planification, la surveillance et la présentation de rapports sur la santé du projet afin de faciliter la prise de décisions en temps opportun.
- « **SPC** » ou « **services de police compétents** » désigne un service de police dont le ressort territorial a été le lieu d'un crime possible ou fait l'objet d'une enquête.
- **« POP »** ou **« prototype sur plateforme »** est un essai de la solution de l'entrepreneur pour confirmer qu'elle fonctionnera tel que décrit dans le modèle de prestation de service d'infonuagique de la solution..
- **« utilisateurs avancés »** désigne un utilisateur dont les compétences et l'expertise sont plus avancées que celles de la plupart des autres utilisateurs, notamment une personne disposant de droits et de responsabilités d'administration liés à la Solution.
- « **CCE »** fait référence aux exigences cotées pour les qualifications de l'entreprise et la gestion du projet.
- « **CFC** » fait référence aux exigences cotées pour les capacités fonctionnelles.
- « **REP** » s'entend des réunions d'examen des progrès, qui ont pour objet d'obtenir une mise à jour sur l'état des activités du projet et de cerner les domaines de problème d'un projet qui nécessitent des mesures de gestion, des décisions ou une transmission aux échelons supérieurs.
- Par « **ordonnance de communication** », on entend une autorisation judiciaire qui oblige une personne, y compris une organisation, à divulguer des documents et des dossiers à un agent de la paix autorisé.

- « **Projet** » signifie un concept d'entreprise plus vaste ou un dossier qui fait appel à davantage de personnel, de partenaires, de temps, de ressources, de résultats et de rapports. Un projet peut contenir des liens vers plusieurs fichiers. Il pourrait servir à gérer les activités et les ressources liées à une campagne spécifique de lutte contre la cybercriminalité ou à un événement important nécessitant une coordination entre plusieurs organismes.
- « **Clôture du projet** » désigne le processus qui comprend les activités suivantes : le client s'assure que le produit ou le travail final est satisfaisant; le client s'assure que le contractant a été payé; le client entame la clôture administrative du contrat, ce qui comprend la vérification des coûts, la modification finale du contrat; enfin, le contrat est clos. Pour de plus amples renseignements, veuillez consulter le chapitre 8 du Guide des approvisionnements de TPSGC : article 8.175 Fin et clôture du contrat[13], ainsi que l'Annexe 8.1 : Lignes directrices sur l'organisation et composition des dossiers d'achat[14] (achatsetventes.gc.ca)[15].
- « **SIRP** » ou « **Système d'incidents et de rapports de police** » désigne le système de gestion des dossiers (SGD) utilisé par la GRC.
- « **Recherche de proximité** » désigne la recherche de deux mots ou plus qui se trouvent les uns par rapport aux autres à l'intérieur d'une certaine limite de mots.
- « **CTC** » désigne les exigences cotées pour les capacités techniques.
- « **CCV** » désigne les exigences cotées pour la démonstration vidéo.
- « **SPAC** », « **Services publics et Approvisionnement Canada** » ou « **Travaux publics et Services gouvernementaux Canada** » fait référence à Services publics et Approvisionnements Canada, comme prévu dans la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*.
- L'« **AQ** » ou « **assurance qualité »** est un moyen d'empêcher les erreurs et les défauts dans les produits fabriqués et d'éviter les problèmes à la prestation de produits ou de services aux clients. La norme ISO 9000 la définit comme « une activité axée sur l'obtention d'une conviction concernant le respect des exigences de qualité »[16].
- On entend par « **CQ** » ou « **Contrôle de la qualité** » le fait de s'assurer que le matériel, les logiciels et les produits livrables répondent aux normes établies par l'entreprise au point de livraison.
- « **RBAC** » ou « **contrôle d'accès basé sur les rôles** » désigne le contrôle d'accès basé sur les rôles des utilisateurs (c.-à-d. un ensemble d'autorisations d'accès qu'un utilisateur reçoit en fonction d'une hypothèse explicite ou implicite sur un rôle donné). Les autorisations selon le rôle peuvent être héritées par une hiérarchie de rôles et reflètent généralement les autorisations nécessaires pour exécuter des fonctions définies au sein d'une organisation. Un rôle donné peut s'appliquer à une seule personne ou à plusieurs personnes (nist.gov).
- « **GRC** » s'entend de la Gendarmerie royale du Canada, qui est le service national de police du Canada et qui assure l'application de la loi au niveau fédéral. La GRC assure également des services de police provinciaux dans huit provinces du Canada (Alberta, Colombie-Britannique, Manitoba, Nouveau-Brunswick, Terre-Neuve-et-Labrador, Nouvelle-Écosse, Île-du-Prince-Édouard et Saskatchewan, c.-à-d. toutes les provinces sauf l'Ontario et le Québec) et des services de police locaux sur une base contractuelle dans les trois territoires (Territoires du Nord-Ouest, Nunavut et Yukon) et dans plus de 150 municipalités, 60 communautés autochtones et trois aéroports internationaux.

---

13 https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-approvisionnements/section/8#section-8.175

14 https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-approvisionnements/section/8#annexe-8.1

15 https://achatsetventes.gc.ca/pour-le-gouvernement/acheter-pour-le-gouvernement-du-canada/administrer-le-contrat/la-cloture-du-dossier-contractuel

16 https://fr.wikipedia.org/wiki/Assurance_qualit%C3%A9

- **« Espace infonuagique de la GRC »** désigne les ressources d'IaaS publiques d'infonuagique Protégé B achetées à un FSI et gérées par la GRC.
- « **SGBDR** » signifie Système de gestion de bases de données relationnelles. Il fait référence à une base de données qui stocke les données dans un format structuré en utilisant des lignes et des colonnes. Il est ainsi facile de localiser des valeurs précises dans la base de données et d'y accéder. Il y a une structure « relationnelle » entre les valeurs de chaque table qui sont liées les unes aux autres. Cette structure permet d'exécuter simultanément des requêtes sur plusieurs tables.
- « **Dossier** » désigne tout document papier ou toute donnée sous format lisible par machine contenant des renseignements personnels ou des données du Canada.
- « **Caviardage** » signifie masquer ou supprimer des parties d'un texte avant sa publication ou distribution.
- « **Red Hat** » est une société de logiciel ouvert.
- « **Regex** » est une expression régulière qui désigne une séquence de caractères définissant un motif de recherche. Ces modèles sont habituellement utilisés par des algorithmes de recherche par chaînes de caractères pour les opérations « rechercher » ou « rechercher et remplacer » sur des chaînes, ou pour la validation des entrées. Il s'agit d'une technique développée en informatique théorique et en théorie des langages formels (Wikipedia.org).
- « **REST** » désigne le transfert d'état représentationnel, qui est un style architectural permettant de fournir des normes entre les systèmes informatiques sur le Web, ce qui facilite ainsi la communication entre les systèmes.
- « **DP** » signifie demande de propositions, qui est un document d'invitation à soumissionner formulée par voie d'appel d'offres, par un organisme intéressé à acheter un produit, un service ou un actif précieux auprès de fournisseurs éventuels afin de soumettre des propositions commerciales.
- « **SGD** » ou « **Système de gestion des dossiers** » désigne un système de TI utilisé par les organismes d'application de la loi pour gérer les événements, les données sur les cas, les enquêtes, les mises en détention de criminels et d'autres données connexes.
- « **OPR** » ou « **objectif du point de reprise** » désigne le temps maximal visé pendant lequel une application peut être arrêtée sans causer de dommages importants à l'entreprise.
- « **ODR** » ou « **objectif du délai de récupération** » désigne la durée pendant laquelle une application peut être arrêtée sans causer de dommages importants à l'entreprise.
- « **SAML** » désigne le langage de balisage d'établissement de la sécurité, une norme ouverte qui permet aux fournisseurs d'identité de transmettre les justificatifs d'identité d'autorisation aux fournisseurs de services. En d'autres termes, un utilisateur peut utiliser un ensemble de justificatifs d'identité pour se connecter à de nombreux sites Web différents.
- « **Bac à sable** » fait référence au « bac à sable » d'analyse des incidents de cybercriminalité du GNCC qui peut être utilisé par les utilisateurs internes de l'Unité, ainsi que par le portail des partenaires et des policiers, dans le but d'effectuer des analyses sur divers fichiers liés à la cybercriminalité.
- « **ESA** » désigne l'évaluation de sécurité et autorisation, qui est le mécanisme par lequel le risque pour un système de TI est compris, atténué et géré de façon constante et mesurable tout au long de son cycle de vie.
- **« SaaS » ou « logiciel en tant que service »** est un modèle de distribution de logiciels dans lequel le client paie par abonnement l'accès à une application qui est hébergée par un fournisseur de services infonuagiques (FSI). Le service est offert sur Internet.
- « **ADNS** » fait référence au projet d'activation et de défense du nuage sécurisé. Son objectif est la mise en œuvre de points d'interconnexion fiables du gouvernement du Canada (GC) à la périphérie du réseau du GC pour l'échange sécurisé de données avec des organismes externes[17].

[17] https://www.canada.ca/fr/services-partages/organisation/publications/2019-2020-plan-ministeriel/tableaux-supplementaires/rapport-etape-project-activation-defense-nuage-securise.html

- « **DCS** » signifie document de conception du système, qui est un produit livrable associé à la solution proposée par le fournisseur.
- « **Registres d'événements de sécurité** » désigne tout événement, toute notification ou alerte qu'un appareil, un système ou un logiciel est techniquement capable de produire en fonction de son état, de ses fonctions et de ses activités. Les registres d'événements de sécurité ne se limitent pas aux appareils de sécurité, mais s'appliquent plutôt à tous les appareils, systèmes et logiciels qui sont techniquement capables de produire des registres d'événements pouvant être utilisés dans les enquêtes de sécurité, l'audit et la surveillance.
- « **Incident de sécurité** » désigne toute anomalie observable ou mesurable survenant à l'égard d'un actif, qui se traduit ou qui peut se traduire par : A) une violation des politiques de sécurité du Canada, d'une mesure de sécurité particulière, des politiques ou procédures de sécurité de l'entrepreneur ou du sous-traitant, ou de toute exigence de ces obligations de sécurité ou des obligations en matière de protection de la vie privée ou B) l'accès non autorisé, la modification ou l'exfiltration de tout justificatif d'identité du personnel autorisé ou de l'utilisateur ou de toute ressource d'information.
- Par « **demande de service** », on entend une demande adressée à l'UNCLC par un organisme partenaire. Certaines demandes de service peuvent être soumises sous forme de transactions structurées par le portail des partenaires et des policiers. De nombreuses demandes de cette nature peuvent être ponctuelles, reçues par courriel, par téléphone, par le portail des partenaires et des policiers, ou produites à l'interne. Voici des exemples de demandes de services :
  - soumettre les données stockées dans le dépôt de la SNC;
  - interroger les données stockées dans le dépôt de la SNC;
  - signaler des données aux fins de surveillance (c.-à-d. BOLO);
  - communiquer un bulletin ou aviser l'UNCLC d'un incident;
  - demander la préservation de données dans une administration étrangère;
  - fournir des conseils ou un accès à de l'expertise;
  - demander une analyse de renseignement;
  - demander de l'aide pour des enquêtes précises sur la cybercriminalité et la fraude;
  - demander l'accès à des outils de logiciel judiciaire pour lutter contre la cybercriminalité et la fraude.
- « **Services** » signifie :
  - accorder des droits d'accès à la solution et d'utilisation de celle-ci;
  - fournir la documentation de la solution;
  - assurer la maintenance, la mise à niveau et la mise à jour de la solution;
  - gérer les incidents et les défauts pour s'assurer que la solution fonctionne au niveau de service applicable;
  - fournir les services d'infrastructure de technologie de l'information accessoires et supplémentaires qui sont nécessaires pour fournir la solution.
- « **GIES** » désigne la gestion de l'information et des événements de sécurité, une sous-section dans le domaine de la sécurité informatique, où les produits et services logiciels combinent la gestion des informations de sécurité (GIS) et la gestion des événements de sécurité (GES). Ils fournissent une analyse en temps réel des alertes de sécurité générées par les applications et le matériel informatique du réseau.
- « **SIENA** » signifie Secure Information Exchange Network Application (Application réseau pour l'échange d'informations sécurisé). SIENA est une plateforme à la fine pointe de la technologie qui répond aux besoins de communication de l'UE en matière d'application de la loi[18].

[18] https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena

- La **« correspondance sans intervention »** signifie que le fournisseur de données recevra une notification électronique automatique d'une requête alors que l'organisme qui fait une requête ne reçoit pas de résultat correspondant dans le résultat d'une requête qui contient des données marquées pour un traitement de correspondance sans intervention.
- « **Requête silencieuse** » désigne une requête qui renvoie une ou plusieurs notifications de corrélation à l'organisme d'interrogation seulement, et non à d'autres organismes comme le fournisseur de données ou les organismes ayant une entrée de liste de surveillance pour l'objet de la requête.
- « **Fonctionnalité d'ouverture unique** » signifie un ensemble de justificatifs d'identité qui permet aux utilisateurs d'accéder à plusieurs applications au sein de votre organisation en ne se connectant qu'une seule fois.
- « **UGS** » ou « **unité de gestion de stock** » est un code de produit qui peut être utilisé pour rechercher et identifier le stock disponible à partir de listes, de factures ou de formulaires de commande. Il est généralement utilisé dans la gestion des stocks.
- « **PME** » ou « **petites et moyennes entreprises** » désigne une entreprise qui, en raison de sa taille, a des besoins informatiques différents et qui fait souvent face à des défis informatiques différents de ceux des grandes entreprises, et dont les ressources informatiques (c.-à-d., généralement son budget et son personnel) sont souvent très limitées (Gartner.com).
- « **EM** » signifie « expert en la matière ».
- « **SMC** » signifie service de messages courts.
- « **SOAP** » signifie Simple Object Access Protocol, qui est une spécification de protocole de messagerie pour l'échange de renseignements structurés dans la mise en œuvre de services Web dans les réseaux informatiques. Son but est de fournir une extensibilité, une neutralité, une verbosité et une indépendance.
- « **Disponibilité de la solution** » désigne le pourcentage de minutes par mois pendant lesquelles la solution est opérationnelle.
- « **Documents techniques de la solution** » désigne tous les manuels, guides d'utilisation et autres documents lisibles par les humains qui sont fournis par l'entrepreneur au Canada aux termes du contrat aux fins d'utilisation avec la solution.
- « **ES** » signifie énoncé de sensibilité
- « **EDT** » signifie le document de l'énoncé des travaux.. Il s'agit de la description narrative de l'exigence de travail d'un projet. Il définit les activités, les produits livrables et les délais propres à un projet pour un fournisseur qui fournit des services au client.
- « **Parole-texte** » est un type de logiciel qui prend réellement du contenu audio et le transcrit en mots écrits dans un traitement de texte ou un autre affichage du numéro demandé. Ce type de logiciel de reconnaissance vocale est extrêmement utile pour quiconque a besoin de générer beaucoup de contenu écrit sans beaucoup de saisie manuelle.
- « **Spécifications** » désigne la description des exigences essentielles, fonctionnelles ou techniques liées aux services dans un énoncé de travail, y compris les procédures permettant de déterminer si les exigences ont été respectées.
- « **SIRPP** » ou « **système d'incidents et de rapports de police protégé** » est une version du SIRP qui offre des fonctions de sécurité améliorées et un accès restreint. Le SIRPP est utilisé pour les incidents liés à la sécurité nationale et aux infrastructures essentielles.
- « **SQL** » désigne le langage d'interrogation structuré, qui est un langage précis au domaine utilisé dans la programmation et conçu pour gérer les données détenues dans un système relationnel de gestion de base de données, ou pour le traitement de flux dans un système relationnel de gestion de flux de données.
- « **MTES** » désigne la matrice de traçabilité des exigences de sécurité. Il s'agit d'un document qui relie les exigences de sécurité du système tout au long du processus de validation. La MTES s'assure que toutes les exigences de sécurité définies pour un système sont mises à l'essai et ne sont pas perdues à l'acceptation finale de la solution.

- « **SPC** » signifie Services partagés Canada, qui est un organisme du gouvernement du Canada chargé de fournir et de consolider les services de technologie de l'information dans tous les ministères fédéraux.
- « **Authentification unique** » signifie un ensemble de justificatifs d'identité qui permet aux utilisateurs d'accéder à plusieurs applications au sein de votre organisation en ne se connectant qu'une seule fois.
- « **STIX** » ou « **Structured Threat Information eXpression** » est un langage structuré et un format de sérialisation utilisé pour échanger des renseignements sur les cybermenaces. Il permet aux organisations d'échanger des renseignements sur les cybermenaces de manière cohérente et lisible par une machine. STIX permet aux communautés de sécurité de mieux comprendre les attaques informatiques qu'ils sont le plus susceptibles de voir et d'anticiper ou de réagir plus efficacement à ces attaques. STIX est conçu pour améliorer de nombreuses capacités différentes comme l'analyse collaborative des menaces, l'échange automatisé des menaces, la détection et l'intervention automatisées, etc.
- « **STT** » ou « **Parole-texte** » est un type de logiciel qui prend réellement du contenu audio et le transcrit en mots écrits dans un traitement de texte ou un autre affichage du numéro demandé. Ce type de logiciel de reconnaissance vocale est extrêmement utile pour quiconque a besoin de générer beaucoup de contenu écrit sans beaucoup de saisie manuelle.
- Les « **présentations** » se rapportent aux présentations de données, aux présentations de renseignements et aux présentations de dossiers de plainte et sont décrites ci-dessous :
  - « **Présentation de données** » s'entend d'une présentation qui contient des renseignements bruts ou des données dans un contexte général, mais qui peut ou non contenir des renseignements pouvant donner lieu à une action. La présentation peut contenir ou non des renseignements accessibles.
  - « **Présentation de renseignements** » (ou « **rens** ») signifie une présentation qui contient des renseignements pouvant donner lieu à une action et qui peut être utilisée sur le plan opérationnel ou renvoyée à un organisme chargé de l'application de la loi. Les présentations de renseignements feront l'objet d'une évaluation d'un analyste du renseignement afin d'en confirmer la fiabilité et la pertinence.
  - « **Présentation d'un dossier de plainte** » désigne une présentation qui est produite par le site Web de signalement public à partir d'un rapport du public ou des petites et moyennes entreprises. Il convient de noter que les rapports publics sur la cybercriminalité et la fraude pourraient aussi provenir de scénarios d'« entrevue » par téléphone entre la victime ou le plaignant et un opérateur du centre d'appel.
- **« Soutien »** fait référence aux quatre (4) niveaux de soutien que la Solution requiert :
  - **Niveau 0** – Demander au super-utilisateur
    - Des solutions automatisées ou en libre-service (p. ex. robots conversationnels) auxquelles les utilisateurs peuvent accéder eux-mêmes sans l'aide du Bureau de service central de la GRC. Il s'agit notamment de la réinitialisation automatique du mot de passe, de la base de connaissances comprenant des renseignements détaillés sur les produits et les techniques et des manuels d'application. Le soutien de niveau 0 est effectué sans l'aide du technicien du Bureau de service central de la GRC.
  - **Niveau 1** – GRC
    - Le Bureau de service central filtre les appels et fournit un soutien et un dépannage de base, notamment la réinitialisation du mot de passe, des instructions pratiques, l'acheminement des billets du gestionnaire du Bureau de service (GBS) vers le soutien de niveau 2 et 3. Un technicien de soutien de niveau 1 recueille de l'information relative au problème de l'utilisateur, l'analyse et détermine la meilleure façon de le résoudre. Le niveau 1 peut également fournir un soutien pour les problèmes relevés aux niveaux 2 et 3 lorsque les solutions de configuration sont documentées. Les foires aux questions (FAQ) et les procédures d'exploitation sont utilisées pour réduire l'acheminement au palier hiérarchique approprié et assurer la formation des utilisateurs.
  - **Niveau 2** – GRC
    - Assure un soutien technique approfondi concernant les problèmes de configuration, le dépannage, l'installation de logiciels, la réparation du matériel, l'administration des bases de

données et l'analyse des causes fondamentales. Traite les problèmes transmis à un niveau supérieur que le technicien de soutien de niveau 1 n'est pas en mesure de traiter. Le technicien peut passer du niveau 2 au niveau 3 lorsque toutes les pistes documentées pour résoudre le problème ont été examinées. Il peut rechercher et mettre en œuvre des solutions à de nouveaux problèmes et ne les acheminer au niveau 3 que si la résolution du problème est au-delà de ses compétences ou de sa capacité.

- **Niveau 3** – GRC/entrepreneur
  - Les experts en la matière tentent de reproduire les problèmes et d'en définir les causes fondamentales, en utilisant les conceptions, le code ou les spécifications des produits, en créant les améliorations, les correctifs et les corrections nécessaires et en assurant la diffusion de versions. Le technicien de soutien de niveau 3 est celui qui possède le plus de compétences en TI et qui est l'expert en la matière le plus à même de résoudre les problèmes non documentés.

- « **ECS** » ou « **échelle de convivialité du système** » est une attitude simple, à dix éléments sur l'échelle de Likert, qui offre une vision globale des évaluations subjectives de la facilité d'utilisation.
- « **SuSE Software und System-Entwicklung** » est un système d'exploitation commercial Linux.
- « **Tâche** » désigne un travail à accomplir ou à entreprendre. Les tâches sont créées et attribuées en tant que demande à une personne ou à une équipe. La personne est alors responsable de l'exécution de la tâche. Les superviseurs gèrent l'avancement d'une tâche jusqu'à son achèvement, sa suspension ou son renvoi, au besoin.
- « **TAXII** » ou « **Trusted Advance eXchange of Indicators Information** » désigne une définition de la façon dont les renseignements sur les cybermenaces peuvent être partagés au moyen de services et d'échanges de messages.
- « **To** » ou « **téraoctet** » est un multiple de l'octet unitaire pour l'information numérique. Le préfixe téra représente la quatrième puissance de 1 000 et donc un téraoctet est un trillion (échelle courte) d'octets.
- « **SCT** » signifie Secrétariat du Conseil du Trésor du Canada. Il fournit des conseils et des recommandations au comité de ministres du Conseil du Trésor sur la façon dont le gouvernement investit dans les programmes et les services, ainsi que sur la façon dont il en assure la réglementation et la gestion.
- **« Ressources de soutien technique »** désigne une resource qui peut fournir des services d'assistance pour résoudre les problèmes liés au système, aux utilisateurs ayant besoin d'une assistance technique ou liée à l'utilisation de la solution.
- « **Billet** » désigne un concept de demande ou de présentation de service qui a été reçu lorsqu'une décision d'agir n'a pas encore été prise. Les billets seront triés pour déterminer leur mandat, leur gravité et leur priorité. Si un billet est exécuté, il devient un fichier. Par exemple :
  - Un billet créé à partir d'un rapport public de faible valeur sera considéré comme une priorité faible et aucune autre mesure ne sera prise – ce rapport public demeurerait un billet.
  - Un analyste peut lier un rapport public évalué à un fichier de renseignements permanent, s'il a été déterminé qu'un lien existe entre le rapport et ce fichier.
  - Une présentation qui est reçue et jugée hautement prioritaire pour l'action de la Section de la coordination opérationnelle sera traitée comme un dossier.
- « **TLP** » ou « **Traffic Light Protocol** » désigne un ensemble de désignations qui sont utilisées pour s'assurer que les renseignements de nature délicate sont partagés avec le public approprié (https://www.us-cert.gov/tlp). Il utilise quatre couleurs pour indiquer les limites de partage attendues à appliquer par le ou les bénéficiaires :
  - **ROUGE** : Les renseignements ne peuvent être divulgués et la distribution est limitée au personnel. Ils ne peuvent être diffusés qu'avec l'accord du propriétaire des données.
  - **ORANGE** : Une communication et une dissémination limitées pour usage officiel uniquement, mais aucune publication ou diffusion dans un lieu public.

- **VERT** : Les renseignements peuvent être partagés avec d'autres personnes, mais ne peuvent être publiés ou affichés sur le Web.
- **BLANC** : Renseignements à l'intention du public. La diffusion se fait sans restriction (publication, affichage sur le Web ou diffusion) et tout membre peut publier les renseignements (sous réserve du droit d'auteur).

- « **TLS** » s'entend de la sécurité de la couche de transport, qui est un protocole cryptographique conçu pour assurer la sécurité des communications sur un réseau informatique.
- « **Recherche par sujet** » ou « **Recherche par descripteur** » signifie que seuls les en-têtes ou les descripteurs de sujet sont recherchés pour des mots qui correspondent à vos termes de recherche. L'utilisation d'en-têtes de sujet permet de s'assurer que tous les éléments d'un même sujet ont des en-têtes cohérents et qu'ils sont tous accessibles à l'aide d'un seul terme de recherche.
- « **EMR** » désigne l'évaluation de la menace et des risques qui consiste à définir les actifs du système et la façon dont ces actifs peuvent être compromis, par l'évaluation du niveau de risque que posent les menaces pour les actifs et la recommandation de mesures de sécurité pour les atténuer.
- « **TTP** » ou « **tactiques, techniques et procédures** » désigne le comportement d'un acteur. Une tactique est le comportement au niveau le plus élevé, tandis que les techniques donnent une description détaillée du comportement dans le contexte d'une tactique, et les procédures offrent une description encore plus détaillée et de plus bas niveau sur le contexte d'une technique.
- « **TXT** » désigne un document texte standard qui contient du texte non formaté.
- « **EAU** » signifie essais d'acceptation par l'utilisateur.
- « **Ubuntu** » est un système d'exploitation ouvert basé sur la distribution Linux Debian.
- « **IU** » ou « **interface utilisateur** » désigne les moyens par lesquels l'utilisateur et un système informatique interagissent.
- « **URL** » signifie localisateur de ressources uniforme.
- « **Utilisateur** » désigne une personne autorisé d'utiliser l'application.
- « **Expérience utilisateur** » fait référence à la réaction d'une personne à l'utilisation d'un produit, d'un système ou d'un service donné. Il décrit généralement la réaction émotionnelle à l'utilisation du système surtout à la lumière de sa facilité d'utilisation ou de la satisfaction qu'il procure.
- « **VERIS** » ou « **Vocabulary for Event Recording and Incident Sharing (vocabulaire pour la consignation d'événements et l'échange de renseignements en matière d'incidents)** » désigne un ensemble de mesures conçues pour fournir un langage commun afin de décrire les incidents de sécurité de manière structurée et répétable.
- « **VIP** » signifie personnalité très importante.
- « **RPV** » signifie réseau privé virtuel. Il déploie un réseau public à l'échelle d'un réseau public et permet aux utilisateurs de transmettre ou de recevoir des données sur des réseaux partagés ou publics, comme si leur ordinateur était connecté directement au réseau privé.
- « **W3C** » ou « **World Wide Web Consortium** » est un regroupement international où les organisations membres, un personnel à temps complet et le public coopèrent à l'élaboration des normes régissant le Web.
- « **Liste de surveillance** » est une liste d'indicateurs de compromis qui peuvent être utilisés pour cerner les présentations sur la cybercriminalité qui présentent un intérêt. Une liste de surveillance peut contenir des valeurs de type observables (par exemple, adresse IP, URL ou nom de domaine), des techniques et processus d'outils de cybercriminalité (par exemple, cheval de Troie, langage de programmation ou enregistreur de clé), des types de crime (par exemple, rançongiciel, fraude du président, minage ou commandement et contrôle) ou d'autres attributs identifiables de cybercriminalité.
- On entend par « **WCAG** » les Règles pour l'accessibilité des contenus Web. Elles ont été élaborées par l'intermédiaire du processus W3C en collaboration avec des particuliers et des organisations des quatre coins du monde, dans le but de présenter une norme commune unique dans le domaine de l'accessibilité

des sites Web qui répond aux besoins des particuliers, des organisations et des gouvernements à l'échelle internationale.

- « **BOEW** » signifie la Boîte à outils de l'expérience Web. Elle comprend des éléments réutilisables permettant de créer et de tenir à jour des sites Web novateurs qui sont accessibles, conviviaux et interopérables. Ces éléments réutilisables sont des logiciels gratuits à source ouverte qui sont utilisés par les ministères du GC et les collectivités Web externes.
- « **WORA** » ou « **écriture unique, exécutable n'importe où** » désigne la capacité d'un programme à être exécuté sur tous les systèmes d'exploitation communs.
- « **Flux des travaux** » désigne la séquence de processus automatisés, manuels, administratifs ou autres par lesquels une tranche de travail passe du début à la fin.
- « **XLSX** » signifie un fichier Microsoft Excel.
- « **XML** » désigne le langage de balisage extensible, qui définit une série de règles pour l'encodage des documents dans un format lisible tant par les humains que par la machine.

ANNEXE E

OBLIGATIONS EN MATIÈRE DE SÉCURITÉ ET PROTECTION DE LA VIE PRIVÉE

1. Vérification de la conformité

(a) Si le Canada doit effectuer des vérifications ou des inspections de sécurité ou examiner d'autres renseignements (p. ex., documents, description de la protection de données, architecture de données et descriptions de sécurité) conformément à la section 12.1, les deux parties conviennent de négocier de bonne foi pour trouver une solution et de tenir compte à la fois de la justification de la demande du Canada et des processus et protocoles de l'entrepreneur.

(b) Dans les 30 jours suivant la demande de l'autorité contractante, l'entrepreneur doit retenir les services d'un tiers pour effectuer une vérification de la protection des renseignements personnels ou fournir des preuves confirmant qu'il ne génère, ne recueille, n'utilise, ne stocke ou ne divulgue aucun renseignement personnel supplémentaire tel que le Canada le définit, autre que les données du client telles que définies par l'entrepreneur, et qu'il n'a pas spécifiquement de renseignements personnels dans les données de soutien (recueillis dans des registres, p. ex., données de télémétrie comme les en-têtes et le contenu des messages électroniques).

2. Propriété des données et demandes de renseignements personnels

(a) Les données sur les clients, y compris tous les renseignements personnels (RP), seront utilisées ou autrement traitées uniquement pour fournir les services, y compris des fins compatibles avec la prestation des services. L'entrepreneur doit s'abstenir d'utiliser ou autrement traiter les données du Canada ou d'en tirer de l'information à des fins publicitaires ou commerciales semblables. Entre les parties, le client conserve tout droit, titre et intérêt relatifs à ses données. L'entrepreneur n'acquiert aucun droit sur les données du Canada, à l'exception des droits que le client accorde à l'entrepreneur pour fournir la solution au client.

(b) Toutes les données que l'entrepreneur stocke, héberge ou traite pour le compte du Canada demeurent la propriété du Canada. À la demande de l'autorité contractante, l'entrepreneur doit fournir des dossiers de renseignements personnels dans les cinq jours ouvrables du gouvernement fédéral (ou sept jours ouvrables du gouvernement fédéral s'ils doivent être récupérés à partir d'une copie ou d'une sauvegarde hors site) dans un document Word ou Excel.

3. Aide dans la prestation d'une évaluation des facteurs relatifs à la vie privée du Canada

(a) À la demande du responsable technique, l'entrepreneur doit aider le Canada à créer une évaluation des facteurs relatifs à la vie privée (EFVP) conformément à la Directive sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor (https://www.statcan.gc.ca/fra/about/pia/dcpia) en aidant le Canada à produire la documentation à l'appui, y compris une EFVP de base pour le Canada fournie par l'entrepreneur. L'entrepreneur convient de fournir ce soutien dans les dix jours ouvrables suivant une demande ou dans un délai convenu d'un commun accord, selon la complexité de la demande par le Canada.

4. Atteinte à la vie privée

(a) L'entrepreneur doit aviser rapidement l'autorité technique (par téléphone et par courriel) de toute compromission ou toute violation ou de tout fait qui amène l'entrepreneur à croire qu'un risque de compromission ou de violation est ou peut être imminent, ou si des mesures de sécurité existantes ont cessé de fonctionner, et ce, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année).

(b) Si l'entrepreneur prend connaissance d'une atteinte à la sécurité entraînant de façon accidentelle ou illégale la destruction, la perte, la modification, la divulgation non autorisée ou l'accès non autorisé aux données ou aux renseignements personnels du client pendant le traitement par l'entrepreneur (chacun étant un « incident de sécurité »), il doit rapidement et sans délai :

(i) aviser le Canada de l'incident de sécurité;

(ii) enquêter sur l'incident de sécurité et fournir au Canada des renseignements détaillés sur cet incident;

(iii) prendre des mesures raisonnables pour atténuer les effets et réduire au minimum les dommages découlant de l'incident de sécurité;

(c) L'entrepreneur doit :

(i) tenir un registre des atteintes à la sécurité avec une description de l'atteinte, la période, les conséquences de l'atteinte, le nom du déclarant et de la personne à qui l'atteinte a été signalée, ainsi que la procédure de récupération des données;

(ii) suivre ou permettre au Canada de suivre les divulgations de données sur le Canada, y compris les données qui ont été divulguées, à qui et à quel moment.

ANNEXE F

PROCESSUS D'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

1. Condition de l'attribution du contrat : Pour obtenir un contrat, le soumissionnaire doit se soumettre avec succès au processus d'intégrité de la chaîne d'approvisionnement (ICA) et ne pas être rejeté.

2. Définitions : Les termes et les expressions utilisés dans le processus d'ICA sont définis de la façon suivante :

    a. « **Données du Canada** » désigne toute donnée provenant des travaux, toute donnée reçu visant à contribuer aux travaux ou générée dans le cadre de la prestation de services de sécurité, de configuration, d'activités, d'administration et de gestion, ainsi que toute donnée transportée ou stockée par l'entrepreneur ou le soustraitant dans le cadre des travaux.
    b. « **Produits** » désigne tout matériel qui fonctionne dans la couche liaison de données du **modèle OSI** (couche 2) ou supérieure, tout logiciel et tout appareil de technologie en milieu de travail.
    c. « **Fabricant du produit** » désigne l'entité qui assemble les composants pour fabriquer le produit final;
    d. « **Éditeur de logiciel** » désigne le propriétaire du logiciel qui a le droit d'octroyer une licence (et d'autoriser d'autres personnes à octroyer une licence ou une sous-licence) pour ses produits logiciels;« **Schéma de la portée de la chaîne d'approvisionnement »** : Un schéma de la portée de la chaîne d'approvisionnement est fourni à l'appendice M afin d'offrir une représentation visuelle des exigences de présentation et d'évaluation de l'Information sur la sécurité de la chaîne d'approvisionnement (ISCA), décrites en détail ci-dessous. En cas d'incompatibilité entre le diagramme et le processus décrit dans ce document, ce dernier a préséance.
    e. **« Information sur la sécurité de la chaîne d'approvisionnement »** désigne tout renseignement que le Canada peut exiger du soumissionnaire ou de l'entrepreneur pour effectuer une évaluation complète de la sécurité de l'ISCA au cours du processus d'ICA.
    f. **« Appareils technologiques en milieu de travail »** désigne les ordinateurs de bureau, les postes de travail mobiles comme les ordinateurs portables et les tablettes, les téléphones intelligents, les téléphones, les périphériques et les accessoires comme les moniteurs, les claviers, les souris, les dispositifs audio et les dispositifs internes et externes de stockage, notamment les clés USB, les cartes à mémoire, les disques durs externes et les CD et DVD inscriptibles.
    g. **« Travaux »** désigne les activités, les services, les biens, l'équipement, la matière et les éléments nécessaires livrés ou réalisés par l'entrepreneur dans le cadre de tout contrat subséquent.

3. **Exigences relatives à la présentation des soumissions** (obligatoires à la date de clôture de la demande de soumissions)

    Les soumissionnaires doivent joindre à leur soumission, au plus tard à la date de clôture de la demande de soumissions, l'ISCA suivante :

    a. **Liste de produits de TI** : Les soumissionnaires doivent indiquer les produits qui pourraient servir à transmettre et à stocker les données du Canada, ou qui pourraient être utilisés ou installés par le soumissionnaire ou un de ses sous-traitants pour effectuer toute partie des travaux, ainsi que les renseignements suivants concernant chaque produit :
        i. **Emplacement** : déterminer à quel endroit chaque produit est interrelié dans tout réseau donné relativement aux données du Canada (indiquer les points de prestation de services ou les nœuds, comme les points de présence, l'emplacement des tiers, les installations de

centres de données, le centre des opérations, le centre des opérations de sécurité, les points d'appairage d'Internet ou d'un autre réseau public, etc.);

ii. **Type de produit** : indiquer la description généralement reconnue par l'industrie pour le matériel, les logiciels, etc. Les composantes d'un produit assemblé, comme un module ou un assemblage de cartes, doivent être fournies pour tous les appareils d'interréseautage de la troisième couche;

iii. **Composant de TI** : indiquer la description généralement reconnue utilisée par l'industrie pour les pare-feu, routeurs, interrupteurs, serveurs, applications de sécurité, etc.;

iv. **Nom ou numéro du modèle du produit** : indiquer le nom ou le numéro du produit attribué par le fabricant;

v. **Description et objectif du produit** : entrer la description ou l'objectif du produit fourni par le fabricant, ainsi que son utilisation ou son rôle prévu dans le cadre des travaux décrits à l'égard du projet;

vi. **Source** : indiquer le fabricant du produit, l'éditeur de logiciel et le fabricant de pièces d'origine des composants intégrés;

vii. **Nom du sous-traitant** : indiquer tous les sous-traitants. Dans le **« Formulaire de présentation de l'ISCA »** fourni avec la demande de soumissions dans le Formulaire 10, « nom du soustraitant » désigne tout sous-traitant qui fournira, installera ou entretiendra un ou plusieurs produits, si le soumissionnaire ne le fait pas lui-même, tel qu'il est précisé ci-dessous.

Il est obligatoire de fournir les renseignements énoncés ci-dessus. Le gouvernement du Canada demande que les soumissionnaires fournissent les renseignements relatifs à la liste des produits de TI au moyen du formulaire d'ISCA, mais le formulaire utilisé pour soumettre lesdits renseignements n'est pas en soi obligatoire. Le Canada demande également que les soumissionnaires indiquent sur chaque page leur dénomination sociale ainsi qu'un numéro de page et le nombre total de pages. Il demande aussi aux soumissionnaires d'insérer une ligne distincte pour chaque produit dans le Formulaire de présentation de l'ISCA. Enfin, le Canada demande aux soumissionnaires de ne pas répéter des itérations multiples du même produit (c.-à-d.,
si le numéro de série ou la couleur sont les seules différences entre les deux produits, ils seront traités comme le même produit aux fins de l'évaluation de l'ISCA.)

b. **Diagrammes de réseau** : Un ou plusieurs diagrammes de réseau conceptuels montrant la totalité du réseau proposé pour la réalisation des travaux décrits dans la présente demande de soumissions. Les diagrammes de réseau doivent uniquement comprendre les portions du réseau du soumissionnaire (et de ceux de ses sous-traitants) sur lesquelles les données du Canada seraient transmises dans le cadre de l'exécution de tout contrat subséquent. À tout le moins, le diagramme doit illustrer ce qui suit :

i. les principaux nœuds suivants servant à la prestation de services dans le cadre de tout contrat subséquent :
   1. les points de service;
   2. le réseau de base;
   3. le ou les réseaux de sous-traitants (préciser le nom du sous-traitant qui figure sur la liste des sous-traitants);

ii. les interconnexions entre les nœuds, s'il y a lieu;

iii. toute interconnexion entre les nœuds et Internet;

iv. pour chaque nœud, un renvoi au produit qui sera déployé dans ce nœud, à l'aide du numéro d'article de la liste des produits de TI.

c. **Liste des sous-traitants** : Le soumissionnaire doit remettre une liste de tous les sous-traitants qui pourraient participer à l'exécution d'une partie des travaux (cela comprend les sous-traitants qui lui sont affiliés ou liés) dans le cadre de tout marché attribué. Au minimum, la liste doit inclure ce qui suit :

i. le nom du sous-traitant;

ii. l'adresse du siège social du sous-traitant;
iii. la partie des travaux que réaliserait le sous-traitant;
iv. le ou les lieux où le sous-traitant réaliserait les travaux.

La liste doit indiquer tous les tiers qui pourraient réaliser une partie des travaux, qu'ils soient des soustraitants du soumissionnaire ou des sous-traitants des sous-traitants du soumissionnaire dans la chaîne d'approvisionnement. Autrement dit, tout sous-traitant qui pourrait avoir accès aux données du gouvernement du Canada ou qui serait responsable du transport ou de l'entreposage de celles-ci doit être nommé. Les sous-traitants comprennent également, par exemple, les techniciens qui pourraient être déployés pour assurer la maintenance de la solution du soumissionnaire. Dans le cadre de cette exigence, un tiers qui fournit des biens au soumissionnaire, mais qui ne réalise pas une partie des travaux, n'est pas considéré comme un sous-traitant. Si le soumissionnaire n'entend pas recourir à des sous-traitants pour réaliser une partie des travaux, le Canada demande qu'il l'indique dans sa soumission.

4. **Évaluation de l'information sur la sécurité de la chaîne d'approvisionnement :**

a. Le Canada déterminera si, à son avis, l'ISCA donne lieu à la possibilité que la solution du soumissionnaire classée au premier rang compromette ou serve à compromettre la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant.

b. Pour ce faire :
   i. le Canada peut exiger du soumissionnaire des renseignements supplémentaires nécessaires pour effectuer une évaluation complète de l'ISCA. Le soumissionnaire disposera de deux jours ouvrables (ou d'un délai plus long précisé par écrit par le Canada) pour fournir les renseignements nécessaires au Canada, à défaut de quoi sa soumission sera rejetée.
   ii. Le Canada peut confier l'évaluation à ses propres ressources ou à des experts conseils et peut, au besoin, se procurer des renseignements supplémentaires auprès de tiers. Le Canada peut utiliser tout renseignement, figurant dans la soumission ou provenant d'une autre source, qu'il juge utile afin d'effectuer une évaluation complète de l'ISCA.

c. Si le Canada juge qu'il est possible que tout aspect de l'ISCA, si celle-ci était utilisée par le Canada, puisse compromettre ou servir à compromettre la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant :

   i. Le Canada écrira (par courriel) au soumissionnaire pour lui faire part des aspects de l'ISCA qui le préoccupent ou qu'il ne peut pas évaluer (par exemple, des versions à venir de produits ne peuvent pas être évaluées). Tous les renseignements supplémentaires que le Canada pourra être en mesure de fournir au soumissionnaire au sujet de ses préoccupations dépendront de la nature de celles-ci. Pour des raisons de sécurité nationale, le Canada ne sera pas toujours en mesure de fournir des renseignements supplémentaires au soumissionnaire. Par conséquent, dans certaines circonstances, le soumissionnaire ne connaîtra pas les raisons sous-jacentes des préoccupations du Canada à l'égard d'un produit, d'un sous-traitant ou d'autres aspects de l'ISCA du soumissionnaire. En ce qui concerne les préoccupations éventuelles, le Canada peut, à son entière discrétion, déterminer une éventuelle mesure d'atténuation que le soumissionnaire pourrait devoir mettre en œuvre par rapport à n'importe quelle portion de l'ISCA si un contrat lui est attribué.

   ii. L'avis donnera au soumissionnaire un minimum de trois (3) occasions de présenter l'ISCA révisée donnant suite aux préoccupations du Canada. Si le Canada a déterminé une mesure d'atténuation que le fournisseur pourrait devoir mettre en œuvre si un contrat lui est attribué, le soumissionnaire doit confirmer dans l'ISCA révisée son consentement ou son refus que tout contrat attribué comprenne des engagements supplémentaires relatifs à

ces conditions d'atténuation. La première ISCA révisée doit être soumise dans les dix (10) jours civils suivant la journée à laquelle l'avis écrit du Canada est envoyé au soumissionnaire (ou un délai plus long précisé par écrit par l'autorité de sécurité de la chaîne d'approvisionnement). Si des préoccupations sont présentées par le Canada au sujet de la première ISCA révisée soumise après la date de clôture des soumissions, la deuxième ISCA révisée devra être présentée dans les cinq (5) jours civils (ou un délai plus long précisé par écrit par l'autorité de sécurité de la chaîne d'approvisionnement). Si des préoccupations sont présentées par le Canada au sujet de la deuxième ISCA révisée soumise après la date de clôture des soumissions, la troisième ISCA révisée devra être présentée dans les trois (3) jours civils (ou un délai plus long précisé par écrit par l'autorité de sécurité de la chaîne d'approvisionnement).

En ce qui a trait à l'ISCA révisée soumise chaque fois, le soumissionnaire doit indiquer dans sa réponse si la révision a une incidence sur tout aspect de sa soumission technique ou de ses attestations. Le soumissionnaire ne sera autorisé à modifier aucun prix dans sa soumission, mais sera autorisé à retirer sa soumission s'il ne veut pas honorer son tarif à la suite de révisions requises à l'ISCA. Chaque fois que le soumissionnaire présentera une ISCA révisée dans le délai imparti, le Canada effectuera une nouvelle évaluation de l'ISCA révisée selon les modalités suivantes :

1. Si le Canada juge qu'il est possible que tout aspect de l'ISCA révisée du soumissionnaire puisse compromettre ou servir à compromettre la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, le soumissionnaire devra recevoir le même type d'avis décrit au paragraphe 4(c), ci-dessus. Si le Canada juge que la troisième ISCA révisée ultérieure à la date de clôture de la demande de soumissions soulève toujours des préoccupations, toute autre occasion de réviser l'ISCA sera à l'entière discrétion du Canada, et la soumission pourrait être rejetée par le Canada en tout temps.

2. Si la soumission n'est pas rejetée par suite de l'évaluation de l'ISCA (révisée conformément au processus indiqué ci-dessus), après la réception de la version finale de l'ISCA révisée, le Canada évaluera l'ensemble des révisions à la soumission technique et aux attestations afin de déterminer si elles ont une incidence sur :
   a. la conformité du soumissionnaire aux exigences obligatoires de la présente demande de soumissions;

   b. la note du soumissionnaire par rapport aux exigences cotées de la présente demande de soumissions, le cas échéant; ou

   c. le classement du soumissionnaire par rapport aux autres soumissionnaires, conformément au processus d'évaluation décrit dans la demande de soumissions.

3. Si le Canada détermine que le soumissionnaire demeure recevable et que son classement par rapport aux autres soumissionnaires n'a pas été touché par les révisions à l'ISCA soumise après la date de clôture des soumissions conformément au processus décrit ci-dessus, l'autorité de sécurité de la chaîne d'approvisionnement recommandera la soumission classée au premier rang pour l'attribution du contrat, sous réserve des dispositions de la demande de soumissions. Si l'approbation du Canada est visée par toute mesure d'atténuation, aucun contrat ne sera attribué au soumissionnaire, à moins que le Canada soit convaincu que le contrat comprend des engagements additionnels reflétant les mesures d'atténuation requises.

4. Si le Canada détermine qu'en raison des révisions à l'ISCA soumises après la date de clôture de la demande de soumissions, conformément au processus décrit ci-dessus, le soumissionnaire n'est plus conforme ou n'est plus classé au premier rang, le Canada procédera à l'examen de la soumission classée au rang suivant pour l'attribution du contrat, toujours sous réserve des dispositions de la demande de soumissions relatives à l'évaluation de l'ISCA soumise à la date de clôture de la demande de soumissions, et à l'évaluation de toute ISCA révisée soumise après la date de clôture de la demande de soumissions, conformément aux dispositions ci-dessus.

d. En participant au présent processus, le soumissionnaire reconnaît que la nature des TI est telle que de nouvelles vulnérabilités, y compris celles liées à la sécurité, sont constamment découvertes. En conséquence :
   i. une évaluation satisfaisante ne signifie pas que la même ISCA ou une ISCA semblable sera évaluée de la même façon pour les besoins futurs;
   ii. au cours de l'exécution de tout contrat subséquent à la présente demande de soumissions, si le Canada est préoccupé par certains produits, conceptions et sous-traitants compris initialement dans l'ISCA, il gérera ses préoccupations conformément aux modalités du contrat.

5. En présentant son ISCA, et compte tenu de la possibilité de participer à ce processus d'approvisionnement, le soumissionnaire accepte les modalités de l'entente de non-divulgation ci-dessous (l'« **entente de nondivulgation** ») :

a. Le soumissionnaire accepte d'assurer la confidentialité et le stockage sécuritaire de toute information qu'il reçoit du Canada au sujet de l'évaluation qu'a faite ce dernier de l'ISCA du soumissionnaire (l'« information de nature délicate »), y compris, sans toutefois s'y limiter, les aspects de l'ISCA qui soulèvent des préoccupations, et les raisons qui ont engendré les préoccupations du Canada à cet égard.

b. L'information de nature délicate comprend notamment les documents, les instructions, les directives, les données, le matériel, les conseils ou autre renseignement, qu'ils soient fournis oralement, par écrit ou autrement, et ce, que cette information soit classifiée, confidentielle, exclusive ou sensible.

c. Le soumissionnaire convient de ne pas reproduire, copier, divulguer, publier ou communiquer, en tout ou en partie, de quelque façon que ce soit, de l'information de nature délicate à une personne autre qu'un employé du soumissionnaire qui a besoin de la connaître et qui détient une attestation de sécurité correspondant à la classification de l'information de nature délicate divulguée, sans recevoir d'abord le consentement écrit de l'autorité de sécurité de la chaîne d'approvisionnement.

d. Le soumissionnaire accepte d'aviser immédiatement l'autorité de sécurité de la chaîne d'approvisionnement dès qu'une personne, autre que celles autorisées en vertu de la sous-section qui précède, accède à de l'information de nature délicate.
e. Le soumissionnaire retenu convient que le non-respect de cette entente de non-divulgation peut entraîner sa disqualification à toute étape du processus d'approvisionnement ou la résiliation immédiate du contrat subséquent ou de tout autre instrument qui en résulte. Le soumissionnaire reconnaît également que toute violation de cette entente de non-divulgation peut entraîner un examen de sa cote de sécurité ainsi qu'un examen de son statut en tant que soumissionnaire admissible pour d'autres besoins.
f. Toute l'information de nature délicate demeure la propriété du Canada et doit être retournée à l'autorité de sécurité de la chaîne d'approvisionnement ou détruite à la demande de cette dernière dans les trente (30) jours suivant cette demande.
g. La présente entente de non-divulgation demeure en vigueur indéfiniment. Si le soumissionnaire souhaite être libéré de ses obligations à l'égard de tous les documents qui contiennent de

l'information de nature délicate, il peut les retourner à un représentant autorisé du Canada, accompagnés d'une référence à la présente entente de non-divulgation. Dans ce cas, toute information de nature délicate connue par le soumissionnaire et son personnel (c.-à-d. l'information de nature délicate qui est connue, mais qui n'est pas consignée par écrit) continuera d'être assujettie à cette entente de non-divulgation, mais il n'y aura aucune autre obligation en ce qui a trait à l'entreposage sécuritaire des documents contenant de l'information de nature délicate (sauf si le soumissionnaire a créé de nouveaux documents contenant de l'information de nature délicate). Le Canada peut demander que le soumissionnaire fournisse la confirmation écrite indiquant que toutes les copies électroniques et papier des documents qui contiennent de l'information de nature délicate ont été renvoyés au Canada.

ANNEXE G

FORMULAIRE D'AUTORISATION DE TÂCHES

APPENDICE A DE L'ANNEXE G

FORMULAIRE D'AUTORISATION DE TÂCHE (AT)			
Entrepreneur		**Numéro de contrat :**	
No d'engagement		**Code financier :**	
No d'autorisation de tâche (modification):		**Date d'émission :**	**Réponse au plus tard le :**

FORMULAIRE D'AUTORISATION DE TÂCHE (AT)

1. Énoncé des travaux (activités, attestations et livrables)

Voir ci-joint l'énoncé des travaux et les attestations requises.

2. Période des services :	**De** (DATE) :		**À** (DATE) :	
3. Emplacement des travaux :				
4. Exigences de déplacement :				
5. Exigences linguistiques :				
6. Autres conditions/contraintes :				
7. Niveau d'attestation de sécurité exigé pour le personnel de l'entrepreneur :				

8. Réponse de l'entrepreneur :

CATÉGORIE ET NOM DE LA RESSOURCE PROPOSÉE	NUMÉRO DE DOSSIER DE SÉCURITÉ DE TPSGC	TAUX QUOTIDIEN	NOMBRE ESTIMATIF DE JOURS	COÛT TOTAL
			Coût estimatif	
			Taxes applicables	
			Total du coût de main-d'oeuvre	
			Total des frais de déplacement et de subsistance	
			Prix ferme ou prix maximum de l'AT	

Signature de l'entrepreneur

Nom, titre et signature de la personne autorisée à signer au nom de **l'entrepreneur** (en caractères d'imprimerie) _____	Signature: _____ Date: _____

FORMULAIRE D'AUTORISATION DE TÂCHE (AT)	
Approval – Signing Authority Approbation - Pouvoir de signature	
Signatures (client) Nom, titre et signature de la personne autorisée à signée : Authorité technique : _____ Date: _____	**Signatures (TPSGC)** Autorité contractante [1]: _____ Date: _____
[1] Signature requise pour les projets d'une valeur de (___)$ ou plus, taxes applicables comprises.	
Vous êtes tenu de vendre à sa Majesté la Reine du Chef du Canada, conformément aux modalités établies ou mentionnées dans la présente ou ci-jointes, les services énumérés dans les présente et dans les documents ci-joints, aux prix établis.	

APPENDICE A DE L'ANNEXE G
ATTESTATIONS À L'ÉTAPE DE L'AUTORISATION DE TÂCHE

Les attestations ci-après doivent être utilisées, le cas échéant. Si elles s'appliquent, elles doivent être signées et jointes à la proposition de l'entrepreneur lorsque celle-ci est soumise au Canada.

1. ATTESTATION RELATIVE AUX ÉTUDES ET À L'EXPÉRIENCE

L'entrepreneur atteste qu'il a vérifié tous les renseignements fournis dans les curriculum vitæ et les documents à l'appui présentés en vue de l'exécution des travaux, plus particulièrement les renseignements relatifs aux études, aux réalisations, à l'expérience et aux antécédents professionnels, et que ceux-ci sont exacts. En outre, le soumissionnaire garantit que chaque personne qu'il a proposée en réponse au besoin est en mesure d'exécuter les travaux prévus par l'AT.

_____ _____

Nom en caractères d'imprimerie de la personne autorisée et signature

Date

2. ATTESTATION DE LA DISPONIBILITÉ DU PERSONNEL

L'entrepreneur atteste que, s'il est autorisé à fournir les services dans le cadre de l'AT, la personne proposée dans son offre de prix pourra commencer les travaux dans un délai raisonnable suivant la date d'attribution de l'AT ou dans le délai précisé dans le formulaire d'AT et qu'elle demeurera disponible pour réaliser le travail requis en réponse au besoin.

_____ _____

Nom en caractères d'imprimerie de la personne autorisée et signature

Date

3. ATTESTATION DU STATUT DU PERSONNEL

Si le soumissionnaire a proposé une personne qui n'est pas un de ses employés, il atteste qu'il a obtenu la permission de cette personne avant d'offrir ses services pour l'exécution des travaux en vertu de l'AT et de soumettre son curriculum vitæ au Canada. Pendant la durée du contrat, le soumissionnaire doit, à la demande de l'autorité contractante, fournir une confirmation écrite, signée par la personne, de la permission donnée au soumissionnaire ainsi que de sa disponibilité. Le défaut de répondre à la demande pourra être considéré comme un manquement en vertu des conditions générales.

_____ _____

Nom en caractères d'imprimerie de la personne autorisée et signature

Date

4. ATTESTATION LINGUISTIQUE

L'entrepreneur atteste que la ressource proposée en réponse à la présente ébauche d'autorisation de tâche peut s'exprimer couramment en anglais. La personne proposée doit être en mesure de communiquer en anglais tant à l'oral qu'à l'écrit, sans aide, et en faisant peu d'erreurs.

_____ _____

Nom en caractères d'imprimerie de la personne autorisée et signature

Date

ANNEXE H

PAIEMENTS PROGRESSIFS

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915	-	155 XL
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
M7594-205915	155xl M7594-205915	

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

Claim for Progress Payment
Demande de paiement progressif

If necessary, use form PWGSC-TPSGC 1112 to record detail costs
Si nécessaire, utiliser le formulaire PWGSC-TPSGC 1112 pour inscrire les coûts détaillés

Contractor's Name and Address Nom et adresse de l'entrepreneur	Claim No. N° de la demande	Date YYYY-MM-DD / AAAA-MM-JJ	Contract Price - Prix contractuel
	File No. - N° du dossier		Contract Serial No. N° de série du contrat

Contractor's Procurement Business Number (PBN) Numéro d'entreprise-approvisionnement (NEA) de l'entrepreneur	Financial Code(s) - Code(s) financier(s)

Contractor's Report of Work Progress (if needed, use additional sheets)
Compte rendu de l'avancement des travaux par l'entrepreneur (si nécessaire, utiliser des feuilles supplémentaires)

Period of work covered by the claim Période des travaux visée par la demande ▶	Current Claim Demande courante		Previous Claims Demandes précédentes		Total to Date Total à date
Description: (Expenditures must be claimed in accordance with the basis and/or method of payment of the contract) **Description :** (Les dépenses doivent être réclamées conformément à la base de paiement et (ou) à la méthode de paiement du contrat).	(A) ☐ 3 decimal	Tax Rate Taux de taxe	(B) ☐ 3 decimal	Tax Rate Taux de taxe	(A + B)
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
Contractor's GST No. N° de TPS de l'entrepreneur	Subtotal Sous-total				
Contractor's QST No. No. de TVQ de l'entrepreneur	Applicable taxes Taxes applicables				
	Total				
	Less holdbacks on expenditures only (Applicable taxes excluded) Moins les retenues sur les dépenses uniquement (Taxes applicables en sus)				

Total Amount of Claim (including applicable taxes)
Montant total de la demande (incluant les taxes applicables)

Percentage of the work completed Pourcentage des travaux achevés	%	Current Claim Demande courante ▶	Amount due Montant dû

PWGSC-TPSGC 1111 (2014-11)

Canada

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915	-	155 XL
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
M7594-205915	155xl M7594-205915	

Claim No. / N° de la demande	Contract Serial No. / N° de série du contrat

CERTIFICATE OF CONTRACTOR

I certify that:

- All authorizations required under the contract have been obtained. The claim is consistent with the progress of the work and is in accordance with the contract.
- Indirect costs have been paid for or accrued in the accounts.
- Direct materials and the subcontracted work have been received, accepted and either paid for or accrued in the accounts following receipt of invoice from supplier/subcontractor, and have been or will be used exclusively for the purpose of the contract.
- All direct labour costs have been paid for or accrued in the accounts and all such costs were incurred exclusively for the purpose of the contract;
- All other direct costs have been paid for or accrued in the accounts following receipt of applicable invoice or expense voucher and all such costs were incurred exclusively for the purpose of the contract; and
- No liens, encumbrances, charges or other claims exist against the work except those which may arise by operation of law such as a lien in the nature of an unpaid contractor's lien and in respect of which a progress payment and/or advance payment has been or will be made by Canada.

ATTESTATION DE L'ENTREPRENEUR

J'atteste que :

- Toutes les autorisations exigées en vertu du contrat ont été obtenues. La demande correspond à l'avancement des travaux et est conforme au contrat.
- Les coûts indirects ont été réglés ou portés aux livres.
- Les matières directes et les travaux de sous-traitance ont été reçus, et le tout a été accepté et payé, ou encore porté aux livres après réception de factures envoyées par le fournisseur ou le sous-traitant; ces matières et ces travaux ont été ou seront utilisés exclusivement aux fins du contrat.
- Tous les coûts de la main-d'oeuvre directe ont été réglés ou portés aux livres et tous ces coûts ont été engagés exclusivement aux fins du contrat.
- Tous les autres coûts indirects ont été réglés ou portés aux livres après réception des factures ou pièces justificatives pertinentes et tous ces coûts ont été engagés exclusivement aux fins du contrat.
- Il n'existe aucun privilège ni demande ou imputation à l'égard de ces travaux sauf ceux qui pourraient survenir par effet de la loi, notamment le privilège d'un entrepreneur non payé à l'égard duquel un paiement progressif et(ou) un paiement anticipé a été ou sera effectué par le Canada.

Contractor 's Signature - Signature de l'entrepreneur	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

Check the box if the claim is being made with respect to advance payment provisions included in the basis of payment of the contract. ☐

Cocher la case si la demande est faite en rapport avec les dispositions relatives aux paiements anticipés qui se trouvent dans la base de paiement du contrat.

This claim, or a portion of this claim, is for an advance payment.

Cette demande, ou une partie de cette demande, est pour un paiement anticipé.

I certify that:

- The funds received will be used solely for the purpose of the contract and attached is a complete description of the purpose to which the advance payment will be applied.
- The amount of the payment is established in accordance with the conditions of the contract.
- The contractor is not in default of its obligations under the contract.
- The payment is related to an identifiable part of the contractual work.

J'atteste que :

- Les fonds reçus ne serviront uniquement qu'aux fins du contrat; ci-joint est une description complète des fins auxquelles le paiement anticipé sera utilisé.
- Le montant du paiement est établi conformément aux conditions du contrat.
- L'entrepreneur n'a pas manqué à ses obligations en vertu du contrat.
- Le paiement porte sur une partie identifiable des travaux précisés dans le contrat.

Contractor 's Signature - Signature de l'entrepreneur	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

CERTIFICATES OF DEPARTMENTAL REPRESENTATIVES

Scientific/Project/Inspection Authority: I certify that the work meets the quality standards required under the contract, and its progress is in accordance with the conditions of the contract.

Inspection Authority (all other contracts): I certify that the quality of the work performed is in accordance with the standards required under the contract.

ATTESTATIONS DES REPRÉSENTANTS DU MINISTÈRE

Autorité scientifique ou responsable du projet / de l'inspection : J'atteste que les travaux sont conformes aux normes de qualité exigées en vertu du contrat et que leur avancement est conforme aux conditions du contrat.

Responsable de l'inspection (tous les autres contrats) : J'atteste que la qualité des travaux exécutés est conforme aux normes exigées en vertu du contrat.

Signature of Scientific / Project / Inspection Authority Signature de l'autorité scientifique ou responsable du projet / de l'inspection	Date (YYYY-MM-DD / AAAA-MM-JJ)

PWGSC Contracting Authority: I certify that, to the best of my knowledge, the claim is consistent with the progress of the work and is in accordance with the contract. This claim, however, may be subject to further verification and any necessary adjustment before final settlement.

Autorité contractante de TPSGC : J'atteste, au meilleur de ma connaissance, que la demande correspond à l'avancement des travaux et est conforme au contrat. Toutefois, cette demande pourrait faire l'objet d'une autre vérification et de tout rajustement nécessaire avant le règlement final.z

Contracting Authority Signature de l'autorité contractante	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

Client's Authorized Signing Officer - (must sign the interim claim): I certify that the claim is in accordance with the contract.

Signataire autorisé du client - (doit signer la demande provisoire) : J'atteste que la demande est conforme au contrat.

Client Signature du client	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

Client's Authorized Signing Officer - (must sign the final claim): I certify that all goods have been received and all services have been rendered, that the work has been properly performed and that the claim is in accordance with the contract.

Signataire autorisé du client - (doit signer la demande finale) : J'atteste que tous les biens ont été reçus, que tous les services ont été rendus, que tous les travaux ont été exécutés convenablement, et que la demande est conforme au contrat.

Client Signature du client	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

ANNEXE I

FORMULAIRES DU SOUMISSIONNAIRE

FORMULAIRE 1 – FORMULAIRES DU SOUMISSIONNAIRE

FORMULAIRE DE PRÉSENTATION DE LA SOUMISSION		
Dénomination sociale du soumissionnaire [***Remarque à l'intention des soumissionnaires :*** *Il incombe aux soumissionnaires qui font partie d'une entreprise de désigner la bonne entreprise*.]		
Représentant autorisé du soumissionnaire aux fins d'évaluation (p. ex., pour des précisions)	Nom	
	Titre	
	Adresse	
	Nº de téléphone	
	Nº de télécopieur	
	Courriel	
Numéro d'entreprise-approvisionnement (NEA) [voir les *Instructions et conditions uniformisées* de 2003] [***Note à l'intention des soumissionnaires:*** *Le NEA donné doit correspondre à la dénomination sociale utilisée dans la soumission. Si ce n'est pas le cas, on établira le soumissionnaire en fonction de la dénomination sociale fournie, et le soumissionnaire devra donner le NEA qui correspond à celle-ci*.]		
Compétence du contrat : Province ou territoire du Canada choisi par le soumissionnaire et qui aura les compétences sur tout contrat subséquent (si différente de celle précisée dans la demande)		

FORMULAIRE DE PRÉSENTATION DE LA SOUMISSION		
Anciens fonctionnaires Voir l'article à la Partie 2 de l'appel d'offre intitulé « Ancien fonctionnaire », pour obtenir une définition pour ancien fonctionnaire.	Le soumissionnaire est-il un ancien fonctionnaire touchant une pension tel que le définit la demande de soumissions? Oui ____ Non ____ Si oui, fournir l'information requise dans la clause de la partie 2, intitulée « Ancien fonctionnaire ».	
	Le soumissionnaire est-il un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu des dispositions de la Directive sur le réaménagement des effectifs? Oui ____ Non ____ Si oui, fournir l'information requise dans la clause de la partie 2, intitulée « Ancien fonctionnaire ».	
Attestation du contenu canadien Comme décrit dans la demande de soumissions, la préférence sera donnée aux soumissions qui auront au moins 80p. 100 de contenu canadien. [Pour obtenir la définition des produits et des services canadiens, consulter la clause K4000D du Guide des CCUA de TPSGC]	En apposant ma signature ci-après, j'atteste au nom du soumissionnaire que [*cocher la case appropriée*] :	
	Au moins 80 p. 100 du prix de la soumission consiste en des produits et services canadiens (comme défini dans la demande de soumissions)	
	Moins de 80 p. 100 du prix de la soumission consiste en des produits et services canadiens (comme défini dans la demande de soumissions)	
Matériel : (*L'autorité contractante devrait seulement l'insérer lorsque les Conditions générales supplémentaires 4001 ont été insérées à la Partie 7.)*	Numéro de téléphone sans frais pour les services de maintenance:	
	Site Web pour les services de maintenance :	
Maintenance et soutien du logiciel sous licence : (*Les autorités contractuelles doivent seulement insérer lorsque la condition générale supplémentaire 4004 a été insérée dans la Partie 7).*	Accès téléphonique sans frais :	
	Accès par télécopieur sans frais :	
	Accès par courriel :	
	Adresse du site Web pour le soutien Web :	

FORMULAIRE DE PRÉSENTATION DE LA SOUMISSION	
Niveau d'attestation de sécurité du soumissionnaire *[indiquer le niveau et la date d'attribution]* ***[Note à l'intention des soumissionnaires :** assurez-vous que le nom dans l'attestation de sécurité correspond à la dénomination sociale du soumissionnaire. Si ce n'est pas le cas, l'attestation n'est pas valide pour le soumissionnaire.]*	
En apposant ma signature ci-après, j'atteste, au nom du soumissionnaire, que j'ai lu la demande de propositions (DP) en entier, y compris les documents incorporés par renvoi dans la DP et que : 1. le soumissionnaire considère qu'il a les compétences et que ses produits sont en mesure de satisfaire les exigences obligatoires décrites dans la demande de soumissions; 2. cette soumission est valide pour la période *exigée* dans la demande de soumissions; 3. tous les renseignements fournis dans la soumissions sont exhaustifs, véridiques et exacts; 4. si un contrat est attribué au soumissionnaire, ce dernier se conformera à toutes les modalités énoncées dans les clauses concernant le contrat subséquent et comprises dans la demande de soumissions.	
Signature du représentant autorisé du soumissionnaire	_____

FORMULAIRE 2 – LETTRE D'ATTESTATION du fournisseur de service infonuagique

Nom du répondant _____

La présente autorisation s'applique au service infonuagique public disponible sur le marché proposé (nom de la solution proposée) :

_____

Le répondant déclare que l'infrastructure et les plateformes sous-jacentes sont hébergées sur un service infonuagique public disponible sur le marché :

La définition de « fournisseur de services infonuagiques » aux fins de cette certification figure à l'annexe D – Définitions et interprétations de la demande de propositions.

Fournisseur de services infonuagiques _____

Lieu du centre de données du fournisseur de services infonuagiques _____

Signature du signataire autorisé du FSI _____

Nom en caractères d'imprimerie du signataire autorisé du FSI _____

Titre en caractères d'imprimerie du signataire autorisé du FSI _____

Adresse du signataire autorisé du FSI _____

Numéro de téléphone du signataire autorisé du FSI _____

Numéro de télécopieur du signataire autorisé du FSI _____

Date de signature _____

FORMULAIRE 3 – FORMULAIRE D'ATTESTATION DE L'ÉDITEUR DE LOGICIELS

Formulaire d'attestation de l'éditeur de logiciel (à utiliser lorsque le soumissionnaire est l'éditeur de logiciel)
Le soumissionnaire atteste qu'il est l'éditeur des logiciels et des composants de logiciel suivants et qu'il a tous les droits requis pour fournir les licences de ces logiciels (et de tous les sous-composants non exclusifs intégrés aux logiciels), libres de redevances pour le Canada :
[*les soumissionnaires devraient ajouter ou retirer des lignes au besoin*]

FORMULAIRE 4 – FORMULAIRE D'AUTORISATION DE L'ÉDITEUR DE LOGICIELS

Formulaire d'autorisation de l'éditeur de logiciel

(à utiliser lorsque le soumissionnaire n'est pas l'éditeur de logiciel)

La présente vise à confirmer que l'éditeur de logiciel identifié ci-dessous a autorisé l'offrant nommé ci-après à fournir des licences de son logiciel dans le cadre du contrat résultant de la demande de soumissions indiquée ci-dessous. L'éditeur de logiciel atteste qu'aucune condition reproduite dans une licence sous emballage rétractable, et reproduite dans ou sur l'emballage du logiciel ou dans toute autre modalité accompagnant le logiciel ne s'appliquera, et que le contrat attribué à la suite de la demande de soumissions (avec ses modifications successives par les parties) représentera l'entente en entier, y compris pour ce qui concerne les licences des produits logiciels de l'éditeur de logiciel indiqués ci-dessous. L'éditeur de logiciel atteste en outre que, si la méthode de livraison (comme le téléchargement) devait nécessiter que l'utilisateur accepte de quelque façon que ce soit l'application de conditions non prévues par la demande de soumissions, ces conditions ne s'appliqueraient pas à l'utilisation par le Canada des produits logiciels de l'éditeur de logiciel indiqués ci-dessous, et ce même si l'utilisateur accepte de quelque façon que ce soit de se soumettre aux conditions supplémentaires.

Cette autorisation s'applique aux logiciels suivants :

_____

_____

[*les soumissionnaires devraient ajouter ou retirer des lignes au besoin*]

Nom de l'éditeur de logiciel (EL) _____

Signature du signataire autorisé de l'EL _____

Nom en caractères d'imprimerie du signataire autorisé de l'EL _____

Titre en caractères d'imprimerie du signataire autorisé de l'EL _____

Adresse du signataire autorisé de l'EL _____

N° de téléphone du signataire autorisé de l'EL _____

N° de télécopieur du signataire autorisé de l'EL _____

Date de signature _____

Numéro de la demande de soumissions _____

Nom du soumissionnaire

FORMULAIRE 5 – FORMULAIRE DE DÉCLARATION

Formulaire de déclaration

Ce formulaire de déclaration doit être soumis dans le cadre du processus de soumission. Veuillez remplir le formulaire et mettre dans une **enveloppe scellée marquée « protéger »** à l'attention d'intégrité, Direction Générale de la Surveillance, TPSGC, 11 rue Laurier, Place du Portage, Phase III, Tour A, 10A1, pièce 108, Gatineau, (Québec) Canada K1A 0S5. Incluez l'enveloppe scellée avec votre présentation de soumission. Le formulaire est désigné « Protégé B » une fois rempli.

Dénomination sociale complète de l'entreprise:	
Adresse de l'entreprise:	
Numéro d'entreprise-approvisionnement de l'entreprise:	
Numéro de la soumission:	
Date de la soumission: (AA-MM-JJ)	

Est-ce que vos sociétés affiliées, un membre de votre conseil d'administration ou vous-même, à titre de soumissionnaire, avez déjà été reconnus coupables d'une infraction au Canada ou d'une infraction similaire à l'étranger ou bien avez déjà plaidé coupable à une telle infraction, en vertu de l'une des dispositions suivantes [1]:

	Oui	Non	Commentaires
Lois sur la gestion des finances publiques 80(1) (d): Fausse inscription, faux certificat ou faux rapport 80(2): Fraude commise au détriment de Sa Majesté 154.01: Fraude commise au détriment de Sa Majesté **Code criminel** 121: Fraudes envers le gouvernement et Entrepreneur qui souscrit à une caisse électorale 124: Achat ou vente d'une charge 380: Fraude commise au détriment de Sa Majesté 418: Vente d'approvisionnement défectueux à Sa Majesté	☐	☐	

Ces 3 dernières années, est-ce que vos sociétés affiliées, un membre de votre conseil d'administration ou vous-même, à titre de soumissionnaire, avez été reconnu coupable d'une infraction au Canada ou d'une infraction similaire à l'étranger ou bien avez plaidé coupable à une telle infraction, en vertu de l'une des dispositions suivantes [1]:

Code criminel 119: Corruption de fonctionnaires judicaires 120: Corruption de fonctionnaires 346: Extorsion De 366 à 368: Faux et infractions similaires 382: Manipulation frauduleuse d'opérations boursières 382.1: Délit d'initié 397: Falsification de livres et de documents 422: Violation criminelle de contrat 426: Commissions secrètes 462.31 Recyclage des produits de la criminalité De 467.11 à 467.13: Participation aux activités d'une organisation criminelle **Loi sur la concurrence** 45: Complot, accord ou arrangement entre concurrents 46: Directives étrangères 47: Truquage d'offres 49: Accords bancaires fixant les intérêts	☐	☐	

[1] Pour lesquelles aucun pardon ou l'équivalent n'a été accordée.

	Oui	Non	Commentaires
52: Indications fausses ou trompeuses 53: Documentation trompeuse			
Loi sur la corruption d'agents publics étrangers 3: Corruption d'agents publics étrangers 4: Comptabilité 5: Infraction commise à l'étranger **Loi réglementant certaines drogues et autres substances** 5: Trafic de substances 6: Importation et exportation 7: Production de substances	☐ ☐	☐ ☐	
Autres Lois 239: Déclarations fausses ou trompeuses (Loi de l'impôt sur le revenu) 327: Déclarations fausses ou trompeuses (Loi sur la taxe d'accise	☐	☐	

Autres commentaires

☐ Je, (nom)_____, (poste)_____, de (nom de l'entreprise-fournisseur)_____ _____ autorise TPSGC à recueillir et à utiliser les renseignements fournis, ainsi que tout autre renseignement dont il pourrait avoir besoin pour déterminer l'inadmissibilité de l'entreprise, et à rendre public les résultats.

☐ Je, (nom) _____, (poste) _____, de (nom de l'entreprise-fournisseur) _____atteste que les renseignements donnés dans le présent formulaire sont, à mes connaissances, véridiques et complètes. De plus, je reconnais que, si des renseignements devraient s'avérer erronés ou manquants, il pourrait en résulter l'annulation de ma soumission, la déclaration de mon admissibilité ou ma suspension.

Nous vous remercions de vouloir faire affaire avec le gouvernement du Canada et de vous montrer compréhensifs quant aux mesures additionnelles que nous devons prendre pour protéger l'intégrité du processus d'approvisionnement de TPSGC.

FORMULAIRE 6 – LISTE DE NOMS

Conformément à la partie 5, article 5.3 – Dispositions relatives à l'intégrité – Liste de noms, veuillez remplir le formulaire ci-dessous.

Dénomination complète de l'entreprise	
Adresse de l'entreprise	
Numéro d'entreprise - approvisionnement (NEA)	
Numéro de l'invitation	
Membres du conseil d'administration (Utilisez le format – Prénom, Nom) Ou mettre la liste en pièce-jointe	
1. Membre	
2. Membre	
3. Membre	
4. Membre	
5. Membre	
6. Membre	
7. Membre	
8. Membre	
9. Membre	
10. Membre	
Autres membres	
Commentaires	

FORMULAIRE 7 (Partie 5) - PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – ATTESTATION

Je, soumissionnaire, en présentant les renseignements suivants à l'autorité contractante, atteste que les renseignements fournis sont exacts à la date indiquée ci-dessous. Les attestations fournies au Canada peuvent faire l'objet d'une vérification à tout moment. Je comprends que le Canada déclarera une soumission non recevable, ou un entrepreneur en situation de défaut, si une attestation est jugée fausse, que ce soit pendant la période d'évaluation des soumissions ou pendant la durée du contrat. Le Canada aura le droit de demander des renseignements supplémentaires pour vérifier les attestations d'un soumissionnaire. Le défaut de se conformer à toute demande ou exigence imposée par le Canada peut également rendre la soumission non recevable ou constituera un défaut en vertu du contrat.

Pour de plus amples renseignements sur le Programme de contrats fédéraux pour l'équité en matière d'emploi, consulter le site Web d'Emploi et Développement social Canada (EDSC) - Travail.

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

Remplir les sections A et B.

A. Cochez seulement l'un des énoncés suivants :

( ) A1. Le soumissionnaire atteste qu'il n'a aucun effectif au Canada.

( ) A2. Le soumissionnaire atteste qu'il est un employeur du secteur public.

( ) A3. Le soumissionnaire atteste qu'il est un employeur sous réglementation fédérale, dans le cadre de la la Loi sur l'équité en matière d'emploi.

( ) A4. Le soumissionnaire atteste qu'il a un effectif combiné de moins de 100 employés permanents à temps plein et/ou permanents à temps partiel au Canada.

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

( ) A5.1. Le soumissionnaire atteste qu'il a conclu un Accord pour la mise en oeuvre de l'équité en matière d'emploi valide et en vigueur avec le Programme du travail de EDSC.

OU

( ) A5.2. Le soumissionnaire atteste qu'il a soumis l'Accord pour la mise en oeuvre de l'équité en matière d'emploi (LAB1168) au Programme du travail de EDSC. Comme il s'agit d'une condition préalable à l'attribution du contrat, remplissez le formulaire intitulé Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168), signez-le en bonne et due forme et transmettez-le aux responsables du Programme du travail de EDSC.

B. Cochez seulement l'un des énoncés suivants :

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

OU

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

FORMULAIRE 8 – FORMULAIRE D'INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE

Comme il est indiqué à la clause 3.1.2 de la partie 3, le soumissionnaire doit déterminer les instruments de paiement électronique qu'il accepte pour le paiement des factures.

Le soumissionnaire accepte les instruments de paiement électronique suivants :

( ) Carte d'achat VISA;

( ) Carte d'achat MasterCard;

( ) Dépôt direct (national et international);

( ) Échange de données informatisé (EDI);

( ) Virement télégraphique (international seulement);

( ) Système de transfert de paiements de grande valeur (plus de 25 M$).

FORMULAIRE 9 – Feuille de présentation de la soumission financière

Les soumissionnaires doivent utiliser les tableaux de prix de l'annexe B - Base de paiement pour remplir leur réponse à la soumission financière.

Tous les prix doivent être indiqués en dollars canadiens, taxes en sus.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915	-	155 XL
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
M7594-205915	155xl M7594-205915	

ANNEXE J

ÉVALUATION TECHNIQUE

CRITÈRES D'ÉVALUATION DES SOUMISSIONS

1. Ce document contient les critères techniques obligatoires et les critères cotés par points qui seront utilisés pour évaluer les solutions proposées par les soumissionnaires pour la Solution nationale en matière de cybercriminalité (SNC).

2. Les soumissionnaires devraient fournir une proposition complète de spécifications techniques et fonctionnelles décrivant en détail comment ils répondent à chacun des critères. Le soumissionnaire devrait faire référence au numéro de la page de sa proposition pour chaque critère soumis.

1.0 CRITÈRES OBLIGATOIRES (CO)

La présente section précise les qualifications du soumissionnaire qui doivent être satisfaites ainsi que les exigences fonctionnelles que la solution doit être en mesure de fournir.

Pour chaque exigence obligatoire, veuillez inclure un renvoi à la page appropriée de votre proposition qui répond à cette exigence. Pour qu'une proposition soit jugée recevable, tous les critères obligatoires doivent être respectés. Les propositions qui ne respectent pas toutes les exigences obligatoires seront rejetées.

1.1 CRITÈRES OBLIGATOIRES SE RAPPORTANT AUX ANTÉCÉDENTS ET AUX QUALIFICATIONS DE L'ENTREPRISE

N° du CO	Description de l'exigence	Conforme		Renvoi (n° de page de la proposition)
		Oui	Non	
Antécédents et expérience de l'entreprise				
CO-1	**Expérience de l'entreprise** Le soumissionnaire doit démontrer qu'il possède les qualifications et l'expérience d'entreprise nécessaires pour fournir la solution et la capacité en matière de ressources pour exécuter les travaux de configuration, d'intégration, de mise à l'essai, de mise en œuvre et de soutien après l'attribution du contrat en fournissant les renseignements suivants : a) Un aperçu de l'organisation de l'entreprise du soumissionnaire, y compris au minimum : i. une description de la structure de l'entreprise; ii. le nombre d'années depuis sa fondation; iii. un aperçu des principales activités opérationnelles; iv. des exemples de principaux clients; v. une estimation récente du nombre d'employés; vi. un aperçu de la présence géographique (emplacements). b) Un historique de l'entreprise en ce qui concerne les produits logiciels, conçus pour aider les organismes d'application de la loi ou gouvernementaux par l'analyse et la coordination opérationnelle entre plusieurs sphères de compétence. c) Une description du lien et de l'expérience du soumissionnaire avec les produits logiciels proposés.			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
	d) Un aperçu des connaissances et de l'expérience du soumissionnaire quant à la mise en œuvre de solutions semblables à la SNC sur le plan de la portée et de la complexité.			
CO-2	**Références pour les projets de l'entreprise** Le soumissionnaire doit démontrer son expérience dans l'exécution de trois (3) contrats pour des organismes gouvernementaux ou privés qui comprennent la configuration, la mise en œuvre et le soutien de solutions semblables en termes de portée et de taille à la SNC. Parmi les trois contrats cités en référence, le soumissionnaire doit inclure un contrat où il a fourni une solution logicielle, conçue pour aider les organismes d'application de la loi ou gouvernementaux par l'analyse, la gestion de cas et la coordination opérationnelle et du renseignement entre plusieurs sphères de compétence. Afin de démontrer cette expérience, le soumissionnaire doit fournir, pour chacun des contrats donnés en référence, les renseignements suivants : a) une description de l'organisation du client; b) le nom et les coordonnées du client (adresse électronique et numéro de téléphone); c) les dates de début et de fin du contrat; d) la valeur du contrat en dollars canadiens; e) une brève description de la portée des travaux et des résultats du contrat; f) le mois et l'année où le produit final a été déployé; g) la taille de l'équipe fournie par le soumissionnaire; h) le statut (p. ex. terminé, annulé ou en cours); i) la taille approximative de la communauté d'utilisateurs; j) si la communauté d'utilisateurs utilise actuellement le produit ou non; k) une brève description des activités du projet liées à l'installation, aux tests, au déploiement, à l'intégration, à la configuration, à la formation et au soutien continu; l) autre information que le soumissionnaire juge appropriée accompagnée d'une indication claire quant à sa pertinence.			
CO-3	**Gestionnaire de projet principal du soumissionnaire**			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
	Le soumissionnaire doit désigner un gestionnaire de projet principal (GPP) qui sera la personne-ressource unique pour tous les aspects de l'exécution du contrat. A. Le GPP doit posséder au moins dix (10) ans (à la date de fermeture de la publication d'appel d'offres) d'expérience en tant que GPP ou chargé de projet pour des projets de GI-TI; B. Le soumissionnaire doit également fournir, pour le candidat, une description de trois (3) grands projets dont ce dernier a supervisé l'exécution au cours des dix (10) dernières années. Pour chaque projet donné en référence, le soumissionnaire doit fournir : a) le nom du projet; b) la valeur du projet; c) la durée du projet; d) les dates où l'engagement de l'entreprise dans le projet a débuté et pris fin; e) les coordonnées du client candidat (p. ex. son nom, son titre, son organisation, son adresse électronique et son numéro de téléphone); f) le rôle du soumissionnaire dans le cadre du projet. Le curriculum vitæ du GPP proposé doit être joint à la soumission.			

3.2 CRITÈRES OBLIGATOIRES SE RAPPORTANT AUX EXIGENCES FONCTIONNELLES

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
Exigences fonctionnelles				
Gestion des cas				
Gestion des billets				
CO-4	La solution proposée par le soumissionnaire doit prendre en charge la création automatique de billets pour toutes les soumissions et les demandes de service reçues par			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
	l'intermédiaire du Portail des partenaires policiers et du portail public ainsi que par courrier électronique, y compris : a. surveillance des soumissions et des demandes de service entrantes pour plusieurs adresses électroniques; b. analyse du contenu, des métadonnées et des indicateurs de compromission des soumissions, des demandes de service et des pièces jointes; c. création automatique d'une valeur de hachage pour chaque courriel et pièce jointe; d. attribution d'un numéro de référence unique à chaque billet.			
Triage et évaluation				
CO-5	La solution proposée par le soumissionnaire doit automatiquement corréler les données des billets avec les données existantes dans le dépôt de données de la SNC, stocker les liens et aviser les utilisateurs, les groupes, les organismes ou les partenaires en matière de cybercriminalité participants en fonction des résultats de la corrélation.			
CO-6	La solution proposée par le soumissionnaire doit utiliser des règles administratives configurables pour déterminer la gravité et la priorité et acheminer automatiquement les billets pour poursuivre leur traitement.			
Files d'attente des travaux				
CO-7	La solution proposée par le soumissionnaire doit prendre en charge la fonctionnalité suivante pour la file d'attente des travaux : a. accès des utilisateurs à leurs tâches et lots de travaux; b. renvoi de tâches et de lots de travaux à des utilisateurs ou des groupes; c. attribution de tâches et de lots de travaux à des utilisateurs ou des groupes; d. recherche, filtrage et tri sur plusieurs attributs de tâches ou de lots de travaux; e. suivi de l'avancement des tâches et des lots de travaux.			
Gestion des billets, des dossiers et des projets				

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO-8	La solution proposée par le soumissionnaire doit prendre en charge la gestion des billets, des dossiers et des projets, y compris ce qui suit : a. Création d'utilisateurs; b. Validation; c. Routage; d. Recherche; e. Affichage; f. Impression; g. Modification; h. Fusion et séparation; i. Division; j. Liaison, dissociation et visualisation des pièces jointes; k. Liaison et dissociation des billets, des fichiers et des projets; l. Gestion des tâches; m. Gestion du statut; n. Gestion de l'historique; o. Renvoi (vers les sections du GNCC ou les partenaires externes); p. Annulation.			
CO-9	La solution proposée par le soumissionnaire doit désigner de manière unique chaque dossier et projet avec un numéro d'identification.			
CO-10	La solution proposée par le soumissionnaire doit permettre à l'utilisateur de créer un « dossier de divulgation » imprimable contenant tout le contenu et les activités liés à un fichier ou un projet, y compris toutes les données liées à la soumission, au billet et aux fichiers, les métadonnées, les journaux d'activité, les journaux de vérification du système et les pièces jointes, permettant ainsi de modifier la configuration, le contenu et la présentation.			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO-11	La solution proposée par le soumissionnaire doit, pour tous les billets, dossiers et projets, inclure les fonctionnalités de regroupement et d'impression suivantes : a. permettre à un utilisateur d'imprimer tout le contenu ou une partie de ce dernier vers une imprimante ou d'en faire une copie électronique imprimable (p. ex. en format PDF); b. permettre à un utilisateur de créer une valeur de hachage pour tout rapport ou toute pièce jointe et de communiquer cette valeur avec le rapport ou la pièce jointe applicable; c. appliquer automatiquement des filigranes configurables de désignation de sécurité de l'information et de protocole de partage aux extrants en fonction des données imprimées, et permettre à un utilisateur de passer outre ou d'appliquer des filigranes manuellement.			
Portail des partenaires policiers (P3)				
CO-12	La solution proposée par le soumissionnaire doit inclure un portail qui fournira aux partenaires externes autorisés et aux organismes d'application de la loi un moyen sécurisé d'accès au système, notamment : a. Recherche dans le dépôt de données de la SNC; b. Envoi de soumissions et de demandes de service en matière de cybercriminalité au GNCC ou à d'autres organismes participant au P3; c. Réception et gestion des notifications, des renvois, des messages et des demandes.			
CO-13	La solution proposée par le soumissionnaire doit permettre à l'utilisateur du P3 de gérer les configurations et les préférences locales, notamment : a. Listes de surveillance; b. Filtres de consultation des fichiers de rapports publics; c. Options de notification; d. Coordonnées.			
Services fonctionnels				

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
Avis				
CO-14	La solution proposée par le soumissionnaire doit prendre en charge les notifications automatiques en temps réel (« alertes ») aux utilisateurs et aux groupes visés en utilisant le courrier électronique et le P3.			
CO-15	La solution proposée par le soumissionnaire doit permettre aux utilisateurs de créer et d'envoyer des notifications et des demandes aux utilisateurs et aux groupes.			
Tableaux de bord				
CO-16	La solution proposée par le soumissionnaire doit offrir des tableaux de bord configurables permettant d'accéder aux notifications, aux messages, aux lots de travaux et aux tâches assignés ainsi qu'à des représentations graphiques de la connaissance de la situation et des rapports opérationnels.			
Analyse de données				
CO-17	La solution proposée par le soumissionnaire doit offrir des capacités automatisées d'analyse des données pour déterminer les tendances, les regroupements et les liens, et produire et transmettre les résultats de la visualisation des données, y compris les tableaux, les graphiques et les cartes géospatiales concernant les liens.			
CO-18	La solution proposée par le soumissionnaire doit permettre à un utilisateur de censurer (bloquer ou cacher les renseignements non communicables) dans un extrant sans supprimer les renseignements du document original.			
Configuration et administration				
CO-19	La solution proposée par le soumissionnaire doit permettre à un utilisateur autorisé de gérer : a. le contenu des tableaux de validation des données et des listes de sélection; b. l'information sur le profil des partenaires et des clients;			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
	c. les modèles, la saisie de données et les notifications; d. les règles régissant le flux de travail.			
Recherche dans le dépôt de la Solution nationale en matière de cybercriminalité (SNC)				
CO-20	La solution proposée par le soumissionnaire doit permettre d'effectuer une recherche fédérée de tout le contenu du dépôt de données de la SNC, structuré et non structuré, y compris les bases de données relationnelles ou non relationnelles, les catalogues de données et les magasins d'objets.			
CO-21	La solution proposée par le soumissionnaire doit pouvoir déclencher des notifications aux parties visées en fonction des corrélations de recherche dans le dépôt de la SNC, notamment : a. faire des recherches dans les données envoyées par un autre organisme; b. faire des recherches dans les données qui figurent sur une liste de surveillance ou dans un « avis de surveillance » (ADS); c. faire des recherches dans les données pour lesquelles un autre organisme a fait des recherches.			
Conserver les règles administratives et les listes de surveillance				
CO-22	La solution proposée par le soumissionnaire doit prendre en charge la gestion des règles administratives configurables utilisées pour : a. déterminer les niveaux de gravité liés aux soumissions; b. déterminer la priorité des demandes de service et des soumissions; c. déterminer les soumissions d'intérêt en fonction des besoins des différentes sections du GNCC, et en établir la priorité; d. établir des listes de surveillance.			
Service de boîte à outils et de base de connaissances en matière de cybercriminalité				

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO-23	La solution proposée par le soumissionnaire doit soutenir la gestion des demandes des partenaires pour accéder aux applications et aux services d'analyse médico-légale en matière de cybercriminalité fournis par le GNCC.			
Intelligence artificielle, apprentissage automatique et traitement du langage naturel				
CO-24	La solution proposée par le soumissionnaire doit pouvoir utiliser le traitement du langage naturel pour extraire du texte et du contenu à partir de données non structurées (texte et images non structurés).			
CO-25	La solution proposée par le soumissionnaire doit pouvoir convertir : a. de l'audio anglais/français et dans d'autres langues que l'anglais/français en texte anglais; b. un texte anglais en texte français ou un texte français en texte anglais; c. du texte dans une autre langue que l'anglais en texte anglais.			
CO-26	La solution proposée par le soumissionnaire doit soutenir les processus de contrôle des résultats de l'intelligence artificielle afin de vérifier la conformité avec la Directive sur la prise de décision automatisée du gouvernement du Canada et d'écarter les résultats involontaires s'il y a lieu.			
Rapports d'aide à la décision				
CO-27	La solution proposée par le soumissionnaire doit permettre aux utilisateurs autorisés de générer des rapports en temps réel à partir de leur bureau, y compris : a. Rapports prédéfinis basés sur des critères de reddition de comptes; b. Rapports spéciaux; c. Rapports de vérification; d. Capacité de sauvegarder les rapports pour les générer plus tard; e. Capacité de sauvegarder et de communiquer les résultats des rapports.			
Référence croisée de logiciels malveillants				

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO-28	La solution proposée par le soumissionnaire doit prendre en charge la gestion des demandes de références croisées de logiciels malveillants, notamment : a. Recevoir des demandes et stocker en toute sécurité des échantillons de logiciels malveillants; b. Établir une correspondance entre les demandes et les échantillons ainsi que les données de la SNC; c. Envoyer des échantillons à des services d'analyse de logiciels malveillants externes sélectionnés; d. Recevoir, stocker et transmettre des rapports d'analyse des logiciels malveillants aux demandeurs.			
Enrichissement automatisé				
CO-29	La solution proposée par le soumissionnaire doit pouvoir lier automatiquement des entités en fonction d'attributs communs, tout en incluant la possibilité d'examiner les entités liées et les liens distincts, le cas échéant. La solution doit également déclencher des notifications selon les liens pour favoriser la résolution des conflits.			
Exigences techniques				
Parole-texte, traduction et reconnaissance optique de caractères				
CO-30	La solution proposée par le soumissionnaire doit fournir un moyen de convertir l'audio en texte ainsi que les images de textes imprimés ou manuscrits en données exploitables par une machine.			
Gestion de l'identité				
CO-31	La solution proposée par le soumissionnaire doit démontrer la prise en charge de la fonctionnalité d'ouverture de session (authentification) pour tous les utilisateurs (y compris le P3), tout en respectant le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3) du gouvernement du Canada.			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO 32	La solution proposée par le soumissionnaire doit pouvoir utiliser la plateforme Azure Active Directory du locataire de la GRC pour l'authentification et la gestion des identités.			
CO 33	La solution proposée par le soumissionnaire doit fournir une fonctionnalité d'ouverture et de fermeture de session unique pour tous les utilisateurs internes. Les partenaires externes (utilisateurs du P3) ne sont pas assujettis à la fonctionnalité d'ouverture et de fermeture de session unique.			
Quarantaine des soumissions				
CO 34	La solution proposée par le soumissionnaire doit inclure la possibilité d'établir et de stocker séparément toutes les soumissions et demandes (y compris les pièces jointes) ayant du contenu malveillant.			
Transfert d'information sécurisé				
CO 35	La solution proposée par le soumissionnaire doit être capable d'échanger en toute sécurité du contenu chiffré par courrier électronique et par le P3.			
Capacité d'importation et d'exportation de données				
CO 36	La solution proposée par le soumissionnaire doit être en mesure d'importer, d'exporter, de décompresser et de comprimer des données, y compris le support pour l'échange sécurisé de fichiers volumineux (fichiers de plus de 1 téraoctet).			
Normes d'échange de données				
CO 37	La solution proposée par le soumissionnaire doit pouvoir échanger des données avec la plateforme d'échange d'information sur les logiciels malveillants.			
Gestion de l'information				
CO 38	La solution proposée par le soumissionnaire doit prendre en charge la gestion et le marquage des documents en utilisant des protocoles d'échange d'information configurables et des désignations de sécurité des données, notamment :			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
	a. Protocole dit des « feux de circulation »; b. Désignations de sécurité concernant l'information du gouvernement du Canada; c. Codes de traitement de l'information d'Europol.			
CO 39	La solution proposée par le soumissionnaire doit prendre en charge les capacités suivantes de gestion du cycle de vie de l'information : a. Gérer la conservation des données selon des calendriers et des dates de conservation et d'élimination configurables; b. Protéger l'information et les données contre les pertes accidentelles et la corruption c. Protéger l'information contre tout accès non autorisé; d. Permettre l'accès à l'information aux groupes et aux utilisateurs en fonction des rôles et des attributs de données assignés (contrôle d'accès en fonction des rôles [RBAC] et contrôle d'accès en fonction des attributs [ABAC]); e. Soutenir la purge automatique et manuelle des données; f. Marquer l'information comme étant retenue; g. Déclencher l'examen, le nouvel étiquetage, l'exportation et la purge de l'information ayant dépassé le niveau de sécurité Protégé B; h. Soutenir l'hébergement des données au Canada.			
Contrôle d'accès en fonction des rôles et des attributs				
CO 40	La solution proposée par le soumissionnaire doit permettre l'utilisation de contrôles d'accès en fonction des rôles (RBAC) et des attributs (ABAC) qui soient configurables afin de limiter l'accès aux fonctionnalités et aux données.			
Intégration				
CO 41	La solution proposée par le soumissionnaire doit permettre l'intégration au système de messagerie électronique de la GRC afin de recevoir et d'envoyer des soumissions et des demandes de service.			

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO 42	La solution proposée par le soumissionnaire doit permettre l'intégration des rapports publics du Système national de signalement des fraudes et de la cybercriminalité (SNSFC) par le biais d'un flux de données.			
CO 43	La solution proposée par le soumissionnaire doit prendre en charge l'intégration avec Esri GIS pour gérer, analyser et échanger les données géospatiales.			
Journal d'activités et de vérification				
CO 44	La solution proposée par le soumissionnaire doit permettre de créer et d'assurer la tenue des journaux immuables d'activité et de vérification de toutes les activités des utilisateurs et du système, y compris : a. Ajout, modification et suppression de données; b. Impression et exportation de données; c. Paramètres de recherche et ensembles de résultats; d. Processus du système; e. Accès des utilisateurs au système; f. Visualisation des journaux par accès en fonction des rôles et des attributs; g. Contenir au minimum ID utilisateur ou ID système, horodatage et activité.			
Clavardage textuel en ligne				
CO 45	La solution proposée par le soumissionnaire doit prendre en charge et gérer les communications sécurisées par clavardage textuel en ligne entre les utilisateurs.			
Publication de documents et productivité				
CO 46	La solution proposée par le soumissionnaire doit prendre en charge les associations d'applications afin de fournir des capacités d'ouverture, de lancement, de visualisation et de modification transparentes relatives aux fichiers joints, y compris les documents et tableurs MS Office et Adobe PDF.			
Facilité d'utilisation				

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO 47	Le soumissionnaire doit décrire comment sa solution est conforme aux normes d'utilisation des systèmes de TI du gouvernement du Canada applicables en matière d'accessibilité et de normalisation des sites Internet, qui sont dérivées des normes WCAG (Web Content Accessibility Guidelines) 2.0 du World Wide Web Consortium (W3C). Consultez : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32620.			
CO 48	La solution du soumissionnaire doit fournir un plan indiquant comment sa solution sera 100% entièrement bilingue (français et anglais) sur toutes les plateformes offertes conformément à la Politique sur les langues officielles du gouvernement du Canada. Cela signifie que les utilisateurs qui choisissent le français ne verront rien en anglais dans l'interface graphique de la solution, y compris, mais sans s'y limiter, dans les fichiers d'aide, les tutoriels, les messages d'erreur et les informations juridiques. (Le contenu généré par l'utilisateur est exclu.) Le soumissionnaire doit également démontrer qu'il fournit fréquemment des services continus de soutien, de maintenance et d'assistance en français et en anglais. Consultez https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26160&section=html.			
CO 49	La solution proposée par le soumissionnaire doit être configurable par l'utilisateur : a. Règles opérationnelles; b. Modèles de saisie et de recherche de données; c. Listes de sélection des données; d. Tableaux de bord.			
Dépôt de données de la SNC				
CO 50	La solution proposée par le soumissionnaire doit prendre en charge un dépôt de données élastiques et évolutives centralisé dans le nuage.			
Besoins non fonctionnels				

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO 51	La solution proposée par le soumissionnaire doit être conçue pour être opérationnelle dans un environnement à disponibilité élevée (disponible en service moyen de 99,45 % sur un mois).			
CO 52	La solution proposée par le soumissionnaire doit pouvoir accepter des changements de taille et de volume avec un minimum d'effort tout en conservant des niveaux de rendement acceptables. Les changements peuvent prendre la forme (mais pas exclusivement) d'un ou plusieurs des éléments suivants : a. Utilisateurs simultanés supplémentaires; b. Emplacements géographiques supplémentaires; c. Organisations partenaires supplémentaires; d. Fonctionnalités supplémentaires; e. Volumes supplémentaires; f. Processus simultanés supplémentaires.			
CO 53	La solution proposée par le soumissionnaire doit accueillir un minimum de 500 utilisateurs simultanément sans diminution du rendement.			
CO 54	La solution proposée par le soumissionnaire doit offrir aux utilisateurs la possibilité de gérer leur mot de passe, conformément aux normes de la GRC, notamment : a. Mot de passe obligatoire pour tous les utilisateurs b. Le mot de passe contient un minimum de 8 caractères, dont un mélange de majuscules et de minuscules et au moins un caractère spécial c. Le changement de mot de passe doit être appliqué lors de la première connexion d'un nouvel utilisateur ou de l'octroi d'un nouveau mot de passe temporaire d. Le changement périodique de mot de passe doit être imposé e. Les utilisateurs doivent pouvoir modifier leur mot de passe à tout moment			
Conformité du fournisseur de service d'infonuagiques au projet d'activation et de défense du nuage sécurisé				

Nº du CO	Description de l'exigence	Conforme		Renvoi (nº de page de la proposition)
		Oui	Non	
CO 55	La solution proposée par le soumissionnaire doit pouvoir être déployée sur une plateforme infonuagique qui a été intégrée avec succès dans le projet d'activation et de défense du nuage sécurisé (ADNS) de SPC et du SCT. Le soumissionnaire doit démontrer sa conformité en fournissant des preuves qui démontrent une intégration réussie entre son programme de sécurité des contrats (PSC) et le réseau du gouvernement du Canada au moyen de l'infrastructure ADNS.			
Soumission vidéo				
CO 56	Le soumissionnaire doit fournir une présentation vidéo narrée (DVD) dans un format de fichier MP4. La présentation vidéo doit démontrer les exigences énoncées dans les capacités obligatoires qui sont indiquées ci-dessous. La présentation vidéo ne doit pas durer plus d'une (1) heure et ne doit pas être une présentation commerciale. La soumission vidéo du soumissionnaire doit appuyer sa soumission écrite et démontrer visiblement les exigences obligatoires suivantes : • CO-04; • CO-05; • CO-07; • CO-08 (de a. à e., inclusivement); and • CO-12.			

4.0 Critères cotés

Les exigences cotées sont des éléments des composantes fonctionnelles, techniques et de gestion de la solution auxquels on attribue des valeurs numériques afin de déterminer les points maximums pouvant être obtenus pour chaque élément. Des exigences cotées sont utilisées pour déterminer le mérite relatif de chaque proposition et la meilleure valeur globale pour le Canada.
Les soumissions seront évaluées et notées en fonction de la note globale la plus élevée. Les points totaux sont indiqués dans le tableau inséré ci-dessous. Chaque critère technique coté doit être traité séparément et doit inclure un renvoi au numéro de page de la proposition aux fins de l'évaluation.

Le tableau suivant résume l'attribution globale de points pour les critères cotés suivants.

Résumé de l'attribution des points

Expérience de l'entreprise et gestion du projet (CCE)	Capacités fonctionnelles (CFC)	Capacités techniques (CTC)	Total
300	1 642	867	2 809
11 %	58 %	31 %	100 %

4.1 Critères organisationnels et critères de gestion cotés

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
Expérience de l'entreprise				
CCE-1	**Expérience de l'entreprise. maximum de 50 points** Le soumissionnaire devrait faire la démonstration des éléments suivants :			
	1. Une à cinq années d'expérience dans la fourniture de solutions logicielles et dans l'exécution de travaux de configuration, d'intégration, de mise en œuvre et de soutien de solutions après l'attribution du contrat. (maximum 5 points)	1 point pour chaque année d'expérience dans la fourniture de solutions logicielles, jusqu'à un maximum de 5 points.		
	2. Plus de cinq années d'expérience dans la fourniture de solutions commerciales et dans l'exécution de travaux de configuration, d'intégration, de mise en œuvre et de soutien de solutions après l'attribution du contrat. (maximum 15 points)	3 points pour chaque année d'expérience au-delà de 5 ans dans la livraison de solutions d'entreprise et l'exécution de travaux de configuration, d'intégration, de mise en œuvre et de support de solutions, jusqu'à un maximum de 15 points.		
	3. Une à cinq années d'expérience dans la fourniture de solutions logicielles, conçues pour aider les organismes d'application de la loi ou gouvernementaux par l'analyse, la gestion des cas et la coordination entre plusieurs sphères de compétence. (maximum 5 points)	1 point pour chaque année d'expérience dans la fourniture de solutions logicielles conçues pour aider les organismes d'application de la loi ou gouvernementaux par l'analyse, la gestion des cas et la coordination entre plusieurs sphères de compétence, jusqu'à un maximum de 5 points.		

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	4. Plus de cinq années d'expérience dans la fourniture de solutions logicielles, conçues pour aider les organismes d'application de la loi ou gouvernementaux par l'analyse, la gestion des cas et la coordination entre plusieurs sphères de compétence. (maximum 15 points)	3 points pour chaque année d'expérience supérieure à 5 ans dans la fourniture de solutions logicielles conçues pour aider les organismes d'application de la loi ou gouvernementaux par l'analyse, la gestion des cas et la coordination entre plusieurs sphères de compétence, jusqu'à un maximum de 15 points.		
	5. Un projet ou plus d'expérience dans la fourniture de solutions liées à la cybercriminalité par l'analyse, le renseignement et la coordination opérationnelle pour un pays du Groupe des cinq (Canada, Australie, Nouvelle-Zélande, le Royaume-Uni et les États-Unis)). (maximum 10 points)	2 points pour chaque projet pertinent cité, jusqu'à un maximum de 10 points.		
CCE-2	**Qualifications et expérience en matière de fourniture de solutions. maximum de 40 points** 1. Le soumissionnaire devrait avoir réalisé au moins un projet de référence comprenant l'installation et le déploiement complets d'une solution logicielle, dans le cadre duquel il a fourni les services professionnels suivants: (maximum 10 points) a) conception; b) mise en œuvre et configuration; c) intégration et interface; d) formation des utilisateurs finaux, des administrateurs de système et du personnel de soutien technique;	2 points pour chaque élément pour un maximum de 10 points		

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	e) soutien à la solution.			
	2. Le soumissionnaire devrait décrire les tâches entreprises pour déployer la solution dans ce projet de référence; (maximum 10 points)	0 point : aucune information ou description incomplète de la manière dont le soumissionnaire répond à l'exigence, ou le soumissionnaire ne répond pas suffisamment à l'exigence; 6 points : description détaillée fournie qui répond suffisamment à l'exigence; 10 points : une description complète et approfondie est fournie, qui répond pleinement à l'exigence et la dépasse.		
	3. La solution employée dans le projet de référence doit être utilisée en ce moment aux fins de la gestion d'enquêtes criminelles et de la production d'extrants d'analyse du début à la fin des enquêtes; (maximum 10 points)	0 point si le projet de référence n'est plus utilisé; 10 points si le projet de référence est toujours utilisé.		
	4. Le soumissionnaire devrait avoir fourni les services professionnels décrits ci-dessus au cours des trois années qui précèdent la date de clôture de la présente DP. (maximum 10 points)	0 point si les services professionnels ne sont pas fournis au cours des trois dernières années; 10 points si les services professionnels ont été fournis au cours des 3 dernières années.		
CCE-3	**Qualifications du gestionnaire de projet principal (GPP). maximum de 50 points**			

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	Le soumissionnaire devrait montrer le nombre d'années au-delà des 10 ans obligatoires pendant lesquelles le ou la GPP dont la candidature est proposée a occupé le poste de gestionnaire principal de projet ou de chef de projet à partir de la clôture de l'appel d'offres et a eu à gérer des projets de GI-TI d'envergure ou à prodiguer des conseils à la haute direction. (Maximum 50 points)	50 points (5 points pour chaque année au-delà des 5 ans obligatoires – jusqu'à un maximum de 10 ans)		
Gestion de projets				
CCE-4	**Calendrier de mise en œuvre de la solution maximum de 40 points** Le soumissionnaire devrait fournir un calendrier de mise en œuvre qui : 1. Décrit ce qui suit : a. le calendrier; b. l'ordre des activités; c. les liens de dépendance; d. les dates de début et de fin; e. les estimations de temps. (maximum 25 points)	5 points pour chaque élément pour un maximum de 25 points		
	2. Décrit l'étendue des travaux, y compris : a. la définition de la portée; b. les jalons; c. les activités;	0 point : aucune information ou description incomplète de la manière dont le soumissionnaire répond à l'exigence, ou le soumissionnaire ne répond pas suffisamment à l'exigence;		

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	d. les livrables.	6 points : description détaillée fournie qui répond suffisamment à l'exigence; 10 points : une description complète et approfondie est fournie, qui répond pleinement à l'exigence et la dépasse.		
	3. Le processus de gestion du calendrier de mise en œuvre et de soutien des calendriers de niveau inférieur à toutes les étapes du cycle de vie de la phase 2.	0 point : aucune information ou description incomplète de l'exigence; 3 points : description détaillée fournie qui répond suffisamment à l'exigence; 5 points : description complète et approfondie qui répond entièrement à l'exigence et la dépasse.		
CCE-5	**Plan d'installation de la solution. maximum de 40 points** Le soumissionnaire devrait fournir un plan préliminaire d'installation de la solution afin de montrer ce qui suit : 1. La compréhension des besoins en matière d'installation de la solution; (maximum 10 points) 2. La façon dont la solution proposée sera mise en œuvre de manière rentable et efficace pour l'étendue complète des travaux définis dans l'EDT, y compris la planification : a. de la configuration; b. de l'intégration;	Pour chaque sous-critère coté: 0 point : aucune information ou description incomplète de la manière dont le soumissionnaire répond à l'exigence, ou le soumissionnaire ne répond pas suffisamment à l'exigence. 6 points : une description détaillée est fournie qui répond suffisamment à l'exigence.		

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	c. de la mise en œuvre; d. des activités de transition. e. du soutien à la solution (maximum 10 points) 3. Des problèmes et risques liés à l'installation, y compris : a. la catégorie; b. la probabilité; c. l'incidence; d. le processus de transmission aux échelons supérieurs; e. les mesures d'atténuation. (maximum 10 points) 4. La contribution prévue du responsable technique de la GRC au processus d'installation de la solution. (maximum 10 points)	10 points : une description complète et approfondie est fournie, qui répond pleinement à l'exigence et la dépasse.		
CCE-6	**Plan de gestion du projet. maximum de 45 points** Le soumissionnaire devrait faire la démonstration des éléments suivants : 1. La façon dont il prévoit gérer l'exécution du contrat et, plus précisément, indiquer les mesures, les processus et le mécanisme qu'il propose de mettre en place pour gérer et fournir les biens et services dans le cadre du contrat final. (maximum 5 points) 2. Le soumissionnaire devrait fournir un organigramme du contrat qui indique la structure de gouvernance du contrat, la structure de l'équipe affectée au contrat, y compris le cadre responsable, le ou la CGPP et le rapport mutuel	Pour chaque sous-critère coté : 0 point : aucune information ou description incomplète de la manière dont le soumissionnaire répond à l'exigence, ou le soumissionnaire ne répond pas suffisamment à l'exigence; 3 points : une description détaillée est fournie qui répond suffisamment à l'exigence;		

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	avec les membres de l'équipe de la GRC. Les rôles et les responsabilités des membres de l'équipe de soumissionnaires doivent être définis. (maximum 5 points)	5 points : une description complète et approfondie est fournie, qui répond pleinement à l'exigence et la dépasse.		
	3. Le soumissionnaire devrait également montrer dans son plan de gestion du projet comment il entend gérer les éléments suivants de la gestion du projet : a. la portée; b. le calendrier; c. le coût; d. la qualité; e. les ressources humaines; f. les communications; g. la gestion de l'information. (5 points maximum pour chaque élément, pour un maximum de 35 points)	5 points maximum pour chaque élément (a, …, g), pour un maximum de 35 points		
CCE-7	**Gestion du changement. maximum de 10 points** Le soumissionnaire devrait fournir un plan de gestion de projet comprenant : 1. l'approche et le processus décrivant la façon dont le soumissionnaire fournira un processus de gestion du changement dans le cadre de sa méthode; (maximum 5 points) 2. les activités et rôles qui entrent en ligne de compte dans la gestion et le contrôle du	Pour chaque sous-critère coté : 0 point : aucune information ou description incomplète de la manière dont le soumissionnaire répond à l'exigence, ou le soumissionnaire ne répond pas suffisamment à l'exigence;		

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	changement pendant l'exécution du contrat. (maximum 5 points)	3 points : une description détaillée est fournie qui répond suffisamment à l'exigence; 5 points : une description complète et approfondie est fournie, qui répond pleinement à l'exigence et la dépasse.		
CCE-8	**Gestion des risques. maximum de 10 points** Le soumissionnaire devrait décrire les sphères de risque liées à la mise en œuvre du projet et la façon dont il entend atténuer, gérer et signaler ces risques pendant la mise en œuvre du projet. (maximum 10)	0 point : aucune information ou description incomplète de la manière dont le soumissionnaire répond à l'exigence, ou le soumissionnaire ne répond pas suffisamment à l'exigence; 6 points : une description détaillée est fournie qui répond suffisamment à l'exigence; 10 points : une description complète et approfondie est fournie, qui répond pleinement à l'exigence et la dépasse.		
CCE-9	**Gestion des problèmes. maximum de 15 points** Le soumissionnaire devrait montrer comment il gérera les problèmes qui peuvent se manifester pendant la mise en œuvre de la SNC. Le plan de gestion des problèmes doit décrire : 1. les questions problématiques possibles liées à la mise en œuvre du projet; (maximum 5 points)	Pour chaque sous-critère coté : 0 point : aucune information ou description incomplète de la manière dont le soumissionnaire répond à l'exigence, ou le soumissionnaire ne répond pas suffisamment à l'exigence;		

Nº du CCE	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
	2. les procédures et processus utilisés pour gérer, signaler et transmettre les problèmes à l'interne et à l'externe au responsable du projet pendant la mise en œuvre du projet; (maximum 5 points) **3.** les procédures et processus à l'aide desquels les questions liées à la mise en œuvre du projet seront transmises à un cadre de l'entreprise désigné aux fins de décision et de résolution. (maximum 5 points)	3 points : une description détaillée est fournie qui répond suffisamment à l'exigence; 5 points : une description complète et approfondie est fournie, qui répond pleinement à l'exigence et la dépasse.		
Qualifications de l'entreprise et gestion du projet - Note totale ▶			**xx/300**	

5.0 Critères fonctionnels cotés

Les soumissions seront évaluées et cotées en fonction du tableau ci-dessous.

Cote	Définition
Exigence démontrée	Explication complète et approfondie de la manière dont le soumissionnaire a démontré qu'il satisfera à l'exigence.
Exigence non démontrée	Explication incomplète ou limitée de la manière dont le soumissionnaire a démontré qu'il satisfera à l'exigence.

Les critères fonctionnels cotés décrivent avec quel degré d'efficacité un entrepreneur peut répondre aux exigences du projet.

5.1 CRITÈRES COTÉS SE RAPPORTANT AUX RAPPORTS DESTINÉS AU PUBLIC

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page la proposition)
Rapports destinés au public				
CFC-1-1	Le soumissionnaire devrait décrire comment la solution qu'il propose traite automatiquement les dossiers de plaintes du public qui ont été saisis par le biais du Système national de signalement des fraudes et de la cybercriminalité (SNSFC).	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
			Rapports destinés au public - Note totale ▶	**xx/10**

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
Capacités de gestion adaptative des cas				
Création de billets				
CFC-2-1	**Réception et analyse des soumissions** Le soumissionnaire devrait décrire comment la solution qu'il propose traite automatiquement toutes les soumissions et demandes de service reçues par courrier électronique, dans le Portail des partenaires policiers (P3) ou à la suite d'une plainte du public, y compris : a. la réception des soumissions et des demandes de service à partir de plusieurs adresses électroniques; b. l'archivage des pièces jointes, de toutes les métadonnées et du courriel original reçus, tels quels; c. la création et le stockage d'une valeur de hachage du courriel et de chaque pièce jointe; d. la conservation d'une copie de toutes les données originales en lecture seule; e. le stockage des données reçues par le biais de gabarits / de champs du P3. L'analyse des données, y compris : f. le corps du courriel; g. les métadonnées; h. les pièces-jointes d'images et de texte, y compris les métadonnées des pièces jointes; i. les pièces jointes structurées, semi-structurées et non structurées.	Maximum de 45 points (5 points par bonne réponse)		
CFC-2-2	Création du billet Le soumissionnaire devrait décrire comment la solution qu'il propose créera et validera automatiquement un billet en fonction du courriel, de la	Maximum de 21 points		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	soumission ou demande du P3 ou de la plainte du public reçue par le biais du SNSFC, y compris : a. la création du billet et la saisie automatique des renseignements dans les champs correspondants; b. la validation des champs obligatoires, des dates, des codes postaux et des champs de province, de ville, de pays; c. l'ajout de pièces jointes au billet; d. l'attribution un identificateur unique au billet; e. la décision quant à savoir si la soumission relève du mandat du GNCC; f. la détermination du type de billet; g. l'acheminement du billet.	(3 points par bonne réponse)		
CFC-2-3	**Gestion du contenu lié à l'exploitation** Le soumissionnaire devrait décrire comment la solution qu'il propose traite le matériel d'exploitation (p. ex. le matériel susceptible d'offenser, comme les images pornographiques d'enfants), y compris : a. la détection du contenu lié à l'exploitation dans les soumissions; b. l'acheminement de telles soumissions aux fins de traitement des exceptions; c. l'élimination du matériel d'exploitation d'une soumission; d. l'acheminement d'une soumission nettoyée en vue de l'achèvement de son traitement.	Maximum de 20 points (5 points par bonne réponse)		
CFC-2-4	**Conversion monétaire** Le soumissionnaire devrait décrire comment la solution qu'il propose fournit un utilitaire de conversion monétaire ayant la capacité de calculer les équivalents en dollars canadiens ($ CA), y compris : a. la conversion de la monnaie fiduciaire; b. la conversion de la cryptomonnaie;	Maximum de 20 points (5 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	c. l'utilisation du taux de conversion actuel; **d.** l'utilisation d'un taux de conversion historique (une date où le cybercrime a eu lieu).			
CFC-2-5	**Examen des billets** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC d'examiner les billets qui ont été créés par la solution, y compris : a. la confirmation de la saisie des champs du billet; b. la modification du billet pour analyser manuellement les entités manquées; c. la suppression des entités analysées par erreur; d. l'apport de corrections au besoin.	Maximum de 20 points (5 points par bonne réponse)		
CFC-2-6	**Gestion des billets** Le soumissionnaire devrait décrire comment la solution qu'il propose permet et favorise la gestion des billets, y compris : a. l'acheminement automatique fondé sur les règles liées au flux de travaux; b. la recherche; c. la modification; d. l'annulation; e. l'ajout de notes en pièces jointes; f. l'ajout des pièces jointes; g. la fusion/séparation; h. la détermination du billet maître; i. la division; j. le réacheminement manuel (p. ex. le réacheminement au superviseur); k. l'impression.	Maximum de 33 points (3 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	Triage et évaluation des soumissions			
CFC-2-7	**Corrélation interne et externe** Le soumissionnaire devrait décrire comment la solution qu'il propose met automatiquement en corrélation les nouvelles données de soumission avec les données existantes dans le dépôt de données cybernétiques de la SNC, ainsi qu'avec les sources externes, et stocke les résultats, y compris : a. le stockage des résultats; b. le classement et la notation des résultats. Les méthodes d'appariement, y compris : c. l'appariement des phrases ou mots exacts; d. l'appariement des mots clés; e. la proximité; f. l'appariement des synonymes; g. l'appariement flou; h. l'appariement des concepts; i. le compte de brouillage; j. correspondance multilingue.	Maximum de 34 points (a. et b. : 5 points par bonne réponse) (de c. à j. : 3 points par bonne réponse)		
CFC-2-8	**Corrélation avancée** Le soumissionnaire devrait décrire comment la solution qu'il propose utilise le traitement du langage naturel pour prendre en charge la corrélation avancée des données, y compris : a. la reconnaissance des sujets et du contenu; b. la détermination du mandat.	Maximum de 20 points (10 points par bonne réponse)		
CFC-2-9	**Fusion des billets et des dossiers**	Exigence démontrée :		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la fusion des billets, des dossiers et des projets confirmés par l'utilisateur en s'appuyant sur la corrélation (dans les cas où un nouveau billet se rattache à un billet, à un dossier ou à un projet existant). La fusion doit être confirmée par un utilisateur.	10 points Exigence non démontrée : 0 point		
CFC-2-10	**Activité d'enrichissement du dépistage et de l'enregistrement** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC d'enregistrer ses activités spéciales liées à l'enrichissement des dossiers, comme les requêtes vers des sources externes ou ouvertes.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-2-11	**Établissement et gestion des notes de gravité** Le soumissionnaire devrait décrire comment la solution qu'il propose permet le calcul automatique de la note de gravité de la soumission, y compris : a. le calcul fondé sur le contenu des soumissions; b. le nouveau calcul itératif, si nécessaire, fondé sur les résultats de chaque activité d'enrichissement; c. l'utilisation de règles administratives configurables de la matrice de gravité; d. l'autorisation d'un utilisateur du GNCC d'outrepasser une note de gravité calculée par le système.	Maximum de 20 points (5 points par bonne réponse)		
CFC-2-12	**Examen des résultats du triage** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC d'examiner l'ensemble des résultats de la totalité des corrélations et des requêtes à des systèmes externes.	Exigence démontrée : 10 points		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
		Exigence non démontrée : 0 point		
CFC-2-13	**Détermination des soumissions présentant un intérêt** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la détermination automatique des soumissions qui présentent un intérêt pour les sections au sein du GNCC et déclenche la signification d'avis nécessaires en tenant compte des éléments suivants : a. les règles administratives relatives à l'établissement des priorités propres à une section; b. les dossiers « en cours »; c. les listes de surveillance propres à chaque section.	Maximum de 15 points (5 points par bonne réponse)		
CFC-2-14	**Acheminement manuel** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge l'acheminement des dossiers, y compris : a. permettre à un utilisateur du GNCC de renvoyer un dossier à une autre section ou à un autre utilisateur du GNCC; b. permettre à un utilisateur du GNCC autorisé de s'approprier un dossier d'une autre section; par exemple, un dossier traité par la section de l'Enregistrement peut être pris en charge par la section du Renseignement en s'appuyant sur la règle administrative relative aux priorités ou sur un avis de corrélation.	Maximum de 10 points (5 points par bonne réponse)		
CFC-2-15	**Détermination des exceptions** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la détermination automatique des dossiers qui nécessitent un traitement des exceptions.	Exigence démontrée : 10 points		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	Les exceptions comprennent les soumissions hors du cadre du mandat, les renseignements insuffisants pour mettre à exécution les règles administratives, le contenu lié aux personnalités de marque, etc.	Exigence non démontrée : 0 point		
	Files d'attente des travaux			
CFC-2-16	**Gestion des lots de travaux** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC : a. d'accéder aux files d'attente des travaux; b. de faire un zoom avant sur les lots de travaux pour accéder aux détails et terminer les tâches; c. de filtrer les lots de travaux en fonction des attributs; d. d'effectuer une recherche un lot de travaux; e. d'effectuer un tri des lots de travaux; f. de consulter les lots de travaux en affichant différents niveaux de détail (p. ex. un dossier dont l'affichage des tâches est visible par rapport à l'affichage d'un résumé du dossier); g. de sauvegarder les préférences en matière d'affichage de la file d'attente des travaux; h. de procéder à l'affectation de lots de travaux; i. de procéder à l'autoaffectation de lots de travaux; j. de réaffecter un lot de travaux à une autre personne ou de remettre un lot de travaux dans un bassin de lots de travaux; k. d'ajouter une note à un lot de travaux; l. d'ajouter une date d'agenda à un lot de travaux; m. de modifier l'état d'un lot de travaux (p. ex. à l'étude, terminé, rejeté).	Maximum de 26 points. (2 points par bonne réponse)		
CFC-2-17	**Flux de travaux mixtes**	Maximum : 9		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge des flux de travaux souples qui permettent les flux de travaux : a. séquentiels, b. parallèles, c. mixtes. Par exemple, une soumission peut être traitée simultanément par trois utilisateurs ou groupes du GNCC différents.	(3 points par bonne réponse)		
	Gestion des dossiers et des projets			
CFC-2-18	**Gestion des dossiers et des projets** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge tous les aspects de la gestion des dossiers et projets au cours d'un cycle de vie complet, y compris : a. la recherche; b. l'affichage; c. l'impression; d. la modification de l'information; e. l'enrichissement; f. l'ajout de notes ou de pièces jointes; g. la création et l'élimination de liens entre les billets et les dossiers, entre les dossiers et les autres dossiers, entre les dossiers et les projets; h. la détermination du dossier maître; i. la gestion des tâches; j. les listes de vérification; k. la gestion des statuts; l. le renvoi;	Maximum de 28 points (2 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	m. la limitation de l'accès en fonction des autorisations du contrôle d'accès basé sur les rôles (RBAC) / du contrôle d'accès basé sur les attributs (ABAC); n. les annulations.			
CFC-2-19	**Aiguillage de dossiers** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge l'aiguillage des billets, des dossiers et des projets aux partenaires extérieurs.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-2-20	**Historique des dossiers** Le soumissionnaire devrait décrire comment sa solution fournit à un utilisateur du GNCC un moyen de gérer, d'accéder et de consulter les versions antérieures des champs ou pièces jointes des billets, dossiers et projets par l'intermédiaire de l'interface utilisateur de la SNC.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-2-21	**Gérer la conservation des données** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la gestion de tous les aspects des dossiers de conservation des données tout au long de leur cycle de vie, y compris : a. La réception d'une demande de conservation des données; b. L'examen et, si nécessaire, la saisie manuelle des demandes de conservation des données; c. La génération de formulaires de demande de conservation avec signature (PDF); d. La gestion de l'état des demandes de conservation; e. La production de demandes de conservation par courrier électronique; f. La saisie des demandes de prolongation de la conservation des données;	Maximum de 40 points (4 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	g. La génération de formulaires d'ordonnance de conservation; h. La délivrance d'ordonnances de conservation par courrier électronique; i. La gestion de l'état des ordonnances de conservation, y compris les renouvellements; j. L'enregistrement du renvoi à un traité d'entraide juridique (TEJ).			
CFC-2-22	Le soumissionnaire devrait décrire comment la solution qu'il propose est en mesure de joindre des fichiers PDF (par exemple, des formulaires de conservation des données, des avis, des rapports sur la connaissance de la situation) aux courriels.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-2-23	Le soumissionnaire devrait décrire comment la solution qu'il propose est capable de prendre en charge l'examen et l'approbation des rapports, avis ou autres résultats (par les utilisateurs autorisés du GNCC) avant la distribution.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-2-24	**Dossier de divulgation** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC de créer un « dossier de divulgation » configurable et imprimable comportant une partie ou la totalité du contenu et des activités liés à un billet, un dossier ou un projet, y compris : a. les données connexes; b. les métadonnées; c. le contenu des registres des activités; d. les journaux de vérification du système; e. les pièces jointes connexes.	Maximum de 10 points (2 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-2-25	**Sortie vers un fichier et impression** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge, pour tous les billets, dossiers et projets, les fonctions de regroupement et d'impression suivantes : a. Permettre à un utilisateur du GNCC d'imprimer la totalité ou une partie du contenu sur une imprimante ou dans une version électronique (p. ex. un fichier PDF, .xls, .doc); b. Appliquer automatiquement des tatouages numériques configurables de désignation de la sécurité de l'information et de partage à l'aide du protocole TLP à toutes les sorties en s'appuyant sur les données imprimées; **c.** Permettre à un utilisateur du GNCC d'appliquer des tatouages numériques configurables à toutes les sorties.	Maximum de 15 points (5 points par bonne réponse)		
CFC-2-26	**Création et gestion des projets** Le soumissionnaire devrait décrire comment sa solution permettra à un utilisateur du GNCC de créer et de gérer des projets, y compris : a. l'attribution d'un numéro de projet unique; b. l'établissement de liens entre un ou plusieurs dossiers et le projet; c. la saisie des détails du projet (p. ex. le nom, le sommaire, la priorité, les dates de début et de fin du projet [unique]); d. l'attribution d'une désignation de sécurité (p. ex. Protégé B); e. l'affectation d'utilisateurs du GNCC et du P3 au projet; f. la gestion des autorisations et des utilisateurs affectés; g. la gestion des parties concernées; h. la gestion de l'état d'avancement du projet; i. la gestion de l'attribution des tâches.	Maximum de 27 points (3 points par bonne réponse)		
Capacités en matière de gestion adaptative des cas – Note totale ▶			**xx/493**	

5.2 CRITÈRES COTÉS SE RAPPORTANT AUX CAPACITÉS DU PORTAIL DES PARTENAIRES POLICIERS (P3)

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
Capacités du Portail des partenaires policiers (P3)				
Interroger la SNC				
CFC-3-1	**Interroger le dépôt de données cybernétiques de la SNC** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 d'interroger le dépôt de données cybernétiques de la SNC, y compris : 1. la fonction de recherche : a. les méthodes de recherche (exacte, floue, de proximité, approximative, de synonymes, par périodes, interlinguistique); b. l'indicateur d'interrogation silencieuse; c. la saisie du motif de la recherche; d. la sauvegarde / le rappel d'une recherche; e. la recherche de notes / le classement des notes; f. l'assurance que les critères obligatoires ont été saisis; g. la création automatique de critères de recherche; 2. Critères de recherche : a. Métadonnées; b. Numéros de référence; c. Créateur des données; d. Indicateurs de compromission; e. Texte non structuré, sujets; f. Types de dossiers (p. ex. demande de service, rapport de plainte du public, conservation des données); g. Lieu où le cybercrime a été commis;	Maximum de 32 points (1a à 1g : 2 points par bonne réponse) (2a à 2i : 2 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	h. Dates (p. ex. date du billet, du dossier ou du projet, date d'ajout de l'information); i. Ciblage de données particulières (p. ex. liste(s) de surveillance, historique des requêtes, corps du courriel ou répertoire complet).			
CFC-3-2	**Affichage des résultats de recherche** Le soumissionnaire devrait décrire comment la solution qu'il propose affiche les résultats de recherche pertinents pour l'utilisateur du P3. Par défaut, les résultats doivent être triés en fonction de leur pertinence par rapport à la requête. La page Résultats de la recherche devrait permettre à l'utilisateur de faire ce qui suit : a. Filtrer; b. Trier; c. Imprimer; d. Afficher les termes de recherche mis en évidence dans le résultat.	Maximum de 12 points (3 points par bonne réponse)		
Présentation d'une demande de service				
CFC-3-3	**Création d'une demande de service** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 de créer divers types de demandes de service en utilisant des modèles d'entrée de données pour faciliter la saisie et la validation des renseignements pertinents en fonction du type de demande. Les demandes de service peuvent être présentées au GNCC ainsi qu'à d'autres organismes utilisateurs du P3 autorisés.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-3-4	**Affichage des accusés de réception et des résultats** Le soumissionnaire devrait décrire comment la solution qu'il propose offre aux utilisateurs du P3 la possibilité d'afficher :	Maximum de 20 points (10 points par		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	a. Les accusés de réception des demandes de service; **b.** Les résultats des demandes de service.	bonne réponse)		
Présentation des renseignements sur la cybercriminalité				
CFC-3-5	**Présentation des renseignements sur la cybercriminalité** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la présentation de renseignements structurés ou non structurés sur la cybercriminalité au GNCC en utilisant le P3, y compris la capacité d'indiquer ce qui suit : a. Contexte de l'information; b. Instructions au GNCC; c. Classification de l'échange de données; d. Désignation de sécurité des données; e. Référence aux soumissions précédentes.	Maximum de 10 points (2 points par bonne réponse)		
CFC-3-6	**Saisie et présentation du dossier de plainte du public** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 de saisir un dossier de plainte de cybercriminalité du public, en utilisant le modèle de saisie de données relatives à une plainte du public, et de le présenter au GNCC aux fins de traitement.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Réception d'avis, de messages et de demandes				
CFC-3-7	**Liste de surveillance du P3** Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge les avis des organismes utilisateurs du P3 en fonction corrélations aux entrées d'une liste de surveillance de l'organisme du P3.	Exigence démontrée : 10 points		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
		Exigence non démontrée : 0 point		
CFC-3-8	**Gestion des messages et des demandes** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à l'utilisateur du P3 : a. de surveiller les demandes et les messages reçus du GNCC ou d'autres organismes utilisateurs du P3; b. de maintenir le statut des messages et des demandes (p. ex. lus, non lus, en cours, répondus, clos); **c.** de créer une réponse structurée à la demande du GNCC qui s'applique.	Maximum de 30 points (10 points par bonne réponse)		
CFC-3-9	**Dossier de mise à jour du P3** Le soumissionnaire devrait décrire comment la solution qu'il propose permettra à un utilisateur du P3 d'exécuter les actions suivantes liées à un billet, à un dossier ou à un projet auquel l'utilisateur du P3 a accès : a. Mise à jour du statut; b. Ajout de notes; c. Ajout de pièces jointes; d. Modification et ajout de données.	Maximum de 12 points (3 points par bonne réponse)		
Accès aux dossiers				
CFC-3-10	**Accès aux rapports destinés au public** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à l'utilisateur du P3 d'accéder aux rapports sur les plaintes du	Maximum de 20 points (10 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	public qui sont mis à la disposition de son service de police compétent, y compris la fourniture : a. d'un accès filtrable et interrogeable; b. d'une indication de la gravité, de la note et de l'enrichissement accru. Les dossiers de plainte du public varieront considérablement en matière de renseignements susceptibles de faire l'objet de mesures. Certains peuvent comprendre l'enrichissement créé par le GNCC, d'autres peuvent ne pas comporter suffisamment de renseignements pour justifier une enquête plus approfondie. La solution devrait, à tout le moins, permettre à l'utilisateur du P3 de faire la distinction entre ces dossiers.			
CFC-3-11	**Renvois de dossiers et de projets** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 d'accéder aux dossiers et aux projets, y compris tous les enrichissements communicables et les renseignements susceptibles de faire l'objet de mesures renvoyés au partenaire du P3 par le GNCC.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-3-12	**Gestion de l'état des dossiers** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à l'utilisateur du P3 de gérer l'état des dossiers en attente afin d'indiquer si le dossier fait ou a fait l'objet d'une mesure et quelle mesure a été prévue ou prise. Cette capacité de gestion de l'état est destinée à fournir au GNCC des renseignements sur les renvois traités par les partenaires du P3.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Enregistrement de la conservation des données				

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-3-13	**Enregistrement de la conservation des données** Le soumissionnaire devrait décrire comment la solution qu'il propose permet la saisie de renseignements relatifs à la conservation des données aux fins d'harmonisation, y compris : a. l'objet de la conservation des données; b. les données à conserver; c. les renseignements sur le détenteur des données; d. l'indicateur de données étrangères ou nationales; e. l'indicateur de demande ou d'ordonnance de conservation (données nationales uniquement); f. les dispositions du *Code criminel* appuyant la conservation des données; g. les dates applicables (début, fin, prolongation); h. le numéro de dossier local et les coordonnées; i. l'indicateur d'ordonnance de production / de traité d'entraide juridique (TEJ).	Maximum de 18 points (2 points par bonne réponse)		
CFC-3-14	**Gestion de la conservation des données enregistrées** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 de gérer la conservation de ses données enregistrées, y compris : a. l'annulation de la conservation; b. l'ajustement des dates et la mise à jour des détails relatifs à la conservation des données enregistrées; **c.** l'indication que la conservation des données a donné lieu à une ordonnance de production.	Maximum de 15 points (5 points par bonne réponse)		
Accès à la base de connaissances / au répertoire				

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-3-15	**Base de connaissances** Le soumissionnaire devrait décrire comment la solution qu'il propose permettra aux utilisateurs du P3 d'accéder à une base de connaissances, y compris : a. la navigation; b. la recherche; c. l'affichage; d. le téléchargement; e. l'impression. La base de connaissances devrait comporter du contenu comme des ressources et des liens éducatifs, des aides à l'emploi et des gabarits, des listes de vérification concernant le recrutement des agents de première ligne, des lignes directrices et des conseils sur les scénarios, ainsi que des précédents et de la jurisprudence.	Maximum de 10 points (2 points par bonne réponse)		
CFC-3-16	**Annuaire des personnes-ressources** Le soumissionnaire doit décrire comment la solution qu'il propose fournit aux utilisateurs du P3 un annuaire consultable des personnes-ressources représentant diverses organisations comme les fournisseurs de services Internet, les services d'échanges de monnaies cryptographiques, les services de sécurité informatique, les experts en matière de cybercriminalité des services d'application de la loi, et des services d'enquêteurs en matière de cybercriminalité et de fraude. Les paramètres de recherche doivent inclure des critères comme l'expertise, le nom de la personne-ressource et le lieu.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-3-17	**Catalogue des outils, des services et des bacs à sable** Le soumissionnaire doit décrire comment la solution qu'il propose permet à un utilisateur du Portail des partenaires policiers (P3) de parcourir, de rechercher, de trouver et de programmer l'utilisation d'outils logiciels accessibles au moyen de la boîte à outils et du bac à sable de lutte contre la cybercriminalité du Groupe national de coordination contre la cybercriminalité (GNCC), notamment : a. effectuer une recherche par type d'outil/fonctions; b. accéder à l'état de disponibilité des outils et au calendrier; c. prévoir du temps pour utiliser un outil.	Maximum de 12 points (4 points par bonne réponse)		
Demande de référence croisée de logiciels malveillants				
CFC-3-18	**Demande de référence croisée de saisie de logiciels malveillants** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 de saisir et de soumettre une demande de référence croisée de logiciels malveillants, y compris : a. le numéro de dossier local; b. un résumé/le contexte; c. l'indicateur d'échantillon de logiciel malveillant à soumettre (soumis séparément); d. les indicateurs de compromission connexes; e. soumis aux fins de renseignement seulement; f. lié à une enquête en cours; g. constatations qui seront utilisées dans le cadre de l'interrogatoire préalable.	Maximum de 14 points (2 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-3-19	**Soumission d'un échantillon de logiciel malveillant** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 de soumettre son échantillon de logiciel malveillant sans mettre en péril l'environnement système du GNCC. La solution devrait permettre de séparer en toute sécurité les échantillons de logiciels malveillants de toutes les données et de tous les systèmes de la Gendarmerie royale du Canada (GRC).	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-3-20	**Examen des résultats de l'analyse des logiciels malveillants** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 d'être informé des résultats de l'analyse de référence croisée des logiciels malveillants, puis d'y accéder.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Gestion des préférences				
CFC-3-21	**Gestion du profil de l'organisme du P3** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur autorisé du P3 de définir des paramètres de configuration propres à l'organisme du P3, notamment : a. Adresse électronique locale pour les notifications; b. Options de notification par courriel (p. ex. toutes les heures, tous les jours, toutes les semaines); c. Coordonnées; d. Profil des capacités; **e.** Organismes connexes – supérieur/subordonné.	Maximum de 10 points (2 points par bonne réponse)		

Nº du CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-3-22	**Gestion de la liste de surveillance du P3** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 de gérer une liste de surveillance (p. ex. liste des indicateurs de compromission, tactiques, techniques et procédures, sujets, BOLO) qui présente un intérêt particulier pour l'organisation de l'utilisateur. La corrélation avec un élément de la liste de surveillance du P3 entraînera, selon les règles relatives à l'avis d'une entrée, l'envoi d'un avis à l'organisme du P3.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-3-23	**Gestion des critères de consultation des rapports publics** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du P3 d'administrer ses paramètres de notification et de visualisation de rapports publics. Ces paramètres permettront à l'organisme du P3 d'adapter ses avis et ses files d'attente pour les rapports publics afin de montrer les rapports qui atteignent ou dépassent les seuils, ou remplissent les « critères d'acceptation » de l'organisme.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Capacité du Portail des partenaires policiers (P3) – Note totale ▶			**xx/315**	

5.3 CRITÈRES COTÉS SE RAPPORTANT AUX CAPACITÉS FONCTIONNELLES

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
Capacités fonctionnelles				
Avis				
CFC-4-1	**Avis automatique** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'envoyer automatiquement des avis aux utilisateurs, aux groupes, aux organismes d'application de la loi ou aux partenaires de lutte contre la cybercriminalité concernés, notamment : • Déclencheurs configurables; • Comptabilité du partage des données, contrôle d'accès fondé sur les rôles et les attributs. Les déclencheurs devraient comprendre la découverte de corrélations – liste de surveillance, requête, nouvelles données ajoutées, modifications de fichiers et renvois de référence.	Maximum de 20 points (10 points par bonne réponse)		
CFC-4-2	**Avis manuel** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNC3 d'envoyer manuellement un avis à : a. un utilisateur; b. un groupe; c. un organisme d'application de la loi; d. un partenaire de lutte contre la cybercriminalité. Le contenu des avis manuels sera également soumis à des restrictions quant à la divulgation.	Maximum de 12 points (3 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-4-3	**Avis par courriel et par message texte** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'envoyer des avis configurables aux utilisateurs du GNCC, aux partenaires de lutte contre la cybercriminalité et aux organismes d'application de la loi par : a. courriel; b. message texte. Dans le cas où un avis hautement prioritaire est envoyé (automatiquement ou manuellement) en dehors des heures de travail, la solution doit permettre d'utiliser le courriel et la messagerie texte pour que l'avis soit transmis en temps réel. Les avis seront autonomes ou indiqueront au destinataire d'accéder au P3 ou au GNCC pour obtenir plus de renseignements.	Maximum de 20 points (10 points pour la capacité de courriel) (10 points pour la capacité de messagerie texte)		
CFC-4-4	**Avis non livrables ou restreints** Le soumissionnaire devrait décrire comment la solution qu'il propose informe un utilisateur du GNCC qu'un avis ne peut être transmis en raison d'une restriction relative au partage de données ou d'une règle de contrôle d'accès fondé sur les rôles ou les attributs.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Tableaux de bord				
CFC-4-5	**Contenu du tableau de bord et analyse descendante** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'utiliser des tableaux de bord configurables du GNCC et du P3, y compris : a. du contenu propre au rôle de l'utilisateur du GNCC et du P3;	Maximum de 36 points (3 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	b. l'accès à des renseignements sommaires sur les avis, les messages, les demandes et les renvois; c. la possibilité de procéder à une analyse descendante des messages, des demandes, et des renvois; d. la recherche, le filtrage et le tri des avis; e. des statistiques des compétences locales; f. des statistiques régionales et nationales; g. des tendances (p. ex. relatives à la victimisation, aux menaces et aux campagnes, tendances thématiques, tendances dans le temps); h. des statistiques et des tendances en matière de fraude et de cybercriminalité : échelles régionale, locale et nationale, avec cartographie thématique; i. les volumes : requêtes, corrélations découvertes; j. les travaux en cours : réception, évaluation, dossiers de renseignement, dossiers de coordination opérationnelle et projets, y compris leur état d'avancement; k. des vignettes illustrant des données cumulatives; **l.** représentations géospatiales et cartes de points chauds.			
CFC-4-6	**Personnalisation du tableau de bord** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC de personnaliser l'affichage de son tableau de bord en choisissant parmi des contenus prédéfinis.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Analyse de données				
CFC-4-7	**Analyse des données**	Maximum de 40 points		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	Le soumissionnaire devrait décrire comment la solution qu'il propose permet à l'utilisateur de travailler dans un environnement interactif et collaboratif de données scientifiques afin de manipuler des données, du code et des modèles associés à diverses sources de données, fichiers et projets, ce qui comprend notamment : a. le stockage temporaire de données (pour fixer un échéancier et tester une hypothèse); b. le nettoyage et la transformation de données; c. la construction de modèles analytiques, écrire du code, l'écriture et l'exécution de code, en tout ou en partie); d. l'application d'un contrôle de versions aux projets d'analyse; e. l'association ou le partage de projets et des données et des modèles qu'ils contiennent avec d'autres utilisateurs et fichiers; f. la découverte de corrélations et de liens et de déclencheurs d'avis connexes, s'il y a lieu; g. l'affichage de données (p. ex. données brutes, données nettoyées, résultats d'exécution de code et résultats des modèles); h. exportation ou association de modèles, de résultats et de projets d'analyse en vue de les partager avec des utilisateurs externes.	(5 points par bonne réponse)		
CFC-4-8	**Affichage des données** Le soumissionnaire devrait décrire comment la solution qu'il propose permet de produire et d'afficher des graphiques et des diagrammes, notamment : a. des diagrammes de liens; b. des organigrammes; c. des graphiques d'événements et des séries chronologiques; d. des cartes géospatiales, des cartes des points chauds, des cartes choroplèthes, densité de points;	25 points maximum (5 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	e. d'autres représentations graphiques des données enrichies par l'outil analytique.			
CFC-4-9	**Enregistrer, afficher et imprimer les résultats d'analyse** Le soumissionnaire doit décrire comment la solution qu'il propose prend en charge des rapports de renseignements complets contenant des représentations graphiques des données et des images, y compris : a. l'enregistrement; b. l'affichage; c. l'impression; d. l'exportation (dans un format de fichier qui peut être exporté, comme le PDF d'Adobe Acrobat)	Maximum de 20 points (5 points par bonne réponse)		
CFC-4-10	**Examiner et communiquer des rapports d'analyse** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur d'examiner et de communiquer des rapports d'analyse, des résultats et des renseignements connexes (état, résultats d'analyse – partiels ou finaux) aux organismes et aux utilisateurs sélectionnés.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-11	**Caviardage** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur de caviarder des renseignements contenus dans des données de sortie afin de protéger des sources ou d'autres personnes qui peuvent être identifiées individuellement et qui ne sont pas le sujet d'un fichier, tout en conservant une version originale non caviardée.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Configuration et administration				

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-4-12	**Vignettes de tableau de bord** Le soumissionnaire devrait décrire comment la solution qu'il propose offre à un utilisateur autorisé du GNCC la possibilité de créer, de modifier et de supprimer des vignettes de tableau de bord qui peuvent être épinglées à des tableaux de bord personnalisés. Les tableaux de bord devraient inclure des autorisations permettant d'adapter le contenu en fonction de différents niveaux d'utilisateurs.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-13	**Gestion de tableaux de code** Le soumissionnaire devrait décrire comment la solution qu'il propose offre à un utilisateur autorisé (administrateur) du GNCC la possibilité de gérer (ajouter, modifier, supprimer) le contenu des tables de codes utilisées à des fins telles que la validation des entrées de données encodées et l'affichage de listes de sélection dans l'interface utilisateur.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-14	**Gestion du contenu de l'aide en ligne** Le soumissionnaire devrait décrire comment la solution qu'il propose offre à un utilisateur autorisé du GNCC la possibilité de gérer le contenu de l'aide en ligne.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-15	**Gestion du répertoire des partenaires et des clients** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur autorisé du GNCC de gérer les renseignements de profil relatifs aux partenaires de lutte contre la cybercriminalité, aux organismes d'application de la loi et à toutes les autres parties prenantes	Maximum de 14 points (2 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	avec lesquelles le GNCC traite. Les profils comprennent des renseignements comme : a. le type de partenaire ou de client; b. le lieu; c. les coordonnées; d. le niveau d'expertise en matière de cybercriminalité; e. les personnes-ressources aux échelons supérieurs et la procédure d'acheminement au palier hiérarchique approprié; f. les préférences en matière de renvoi des organismes d'application de la loi; g. les seuils.			
CFC-4-16	**Gérer l'annuaire des personnes-ressources** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur autorisé du GNCC de gérer les coordonnées des ressources et des experts en matière de cybercriminalité qui seront mises à la disposition de la police et des partenaires sur le P3, notamment : a. Création b. Modification c. Suppression d. Recherche e. Tri et filtre	Maximum de 10 points (2 points par bonne réponse)		
CFC-4-17	**Gestion des modèles et des règles** Le soumissionnaire devrait décrire comment la solution qu'il propose permet de gérer des modèles et des règles, notamment : a. la gestion et la modification des modèles de notification, y compris le contenu et les autorisations;	Maximum de 20 points (5 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	b. la configuration des modèles de réponse du P3; c. la configuration des modèles de soumission du P3; d. les règles relatives à la configuration des modes de notification; indiquer quand le P3 doit envoyer un courriel, un message texte ou un avis (ou toute combinaison de ces moyens de communication).			
CFC-4-18	**Création et gestion des flux de travail** Le soumissionnaire devrait décrire comment la solution qu'il propose offre à un utilisateur autorisé du GNCC la possibilité de gérer les flux de travail, ce qui comprend notamment : a. la création de flux de travail; b. la définition et la gestion du routage; c. la définition et la gestion des tâches; d. la définition des groupes d'utilisateurs concernés.	Maximum de 20 points (5 points par bonne réponse)		
Recherche dans le répertoire de données de la Solution nationale en matière de cybercriminalité (SNC)				
CFC-4-19	**Recherche dans la SNC** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'effectuer des recherches sur un champ ou un attribut applicable dans le répertoire de données de la SNC. Si l'on utilise plus d'un critère, la solution par défaut devrait produire des résultats qui remplissent tous les critères (selon la méthode de recherche choisie).	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-20	**Techniques avancées de recherche** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'employer les différentes méthodes de recherche suivantes : a. Mots, expressions ou sujets exacts qui répondent aux critères; b. Recherche par opérateurs de proximité;	Maximum de 26 points. (2 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	c. Recherche par opérateurs de proximité dans des phrases ou des paragraphes; d. Recherches avec caractères de remplacement; e. Recherche booléenne; f. Synonymes des mots utilisés dans les critères de recherche; g. Recherche floue (p. ex. Soundex); h. Mots brouillés (p. ex. disco= d1$c0, monsite.com = monsite point com); i. Recherche multilingue; j. Recherche par mots-clés; k. Recherche conceptuelle; l. Possibilité d'utiliser du texte dans une langue étrangère et recherche multilingue; m. Toute combinaison de critères de recherche indiqués ci-dessus dans une même requête.			
CFC-4-21	**Classement des résultats de recherche** Le soumissionnaire devrait décrire comment la solution qu'il propose génère une note pour chaque résultat qui est présenté à l'utilisateur et qui indique son degré de correspondance aux critères de la requête.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-22	**Contenu des résultats de recherche** Le soumissionnaire devrait décrire comment la solution qu'il propose fournit des résultats de recherche pertinents, ce qui comprend les caractéristiques suivantes : a. Classement des résultats (note); b. Ordre de tri par défaut (p. ex. résultat, date correspondante ou ordre alphabétique [le cas échéant]); c. Type de correspondance (exacte, proximité);	Maximum de 30 points (5 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	d. Données correspondant à (p. ex. historique des requêtes, conservation des données, soumission des données, dossier de plainte); e. Renseignements sur la date des résultats (p. ex. date, date d'ajout des données, date de la dernière mise à jour); f. Coordonnées.			
CFC-4-23	**Fonctions d'affichage des résultats** Le soumissionnaire devrait décrire comment la solution qu'il propose offre aux utilisateurs la possibilité de : a. filtrer les résultats; b. trier les résultats; c. faire une analyse descendante, ascendante ou transversale pour afficher les détails (p. ex. un bon de travail ou un fichier).	Maximum de 15 points (5 points par bonne réponse)		
CFC-4-24	**Interface de requête en langue naturelle** Le soumissionnaire devrait décrire comment la solution qu'il propose fournit aux utilisateurs une interface de requête en langue naturelle, ce qui comprend les caractéristiques suivantes : a. Ligne de commande (saisie de requête); b. Formulaire et modèle (champs à remplir); c. Assistance graphique (glisser-déposer ou sélectionner une région géographique).	Maximum de 15 points (5 points par bonne réponse)		
CFC-4-25	**Enregistrement des critères de recherche** Le soumissionnaire devrait décrire comment la solution qu'il propose offre à l'utilisateur la possibilité d'enregistrer les critères de recherche en vue d'une utilisation ultérieure, y compris la capacité de faire ce qui suit : a. Nommer une recherche; b. Accéder à un historique de recherche par nom, date, critères;	Maximum de 15 points (5 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	c. Transmettre une recherche à d'autres utilisateurs.			
CFC-4-26	**Requête silencieuse** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'effectuer une requête silencieuse. La solution doit respecter les règles d'interrogation silencieuse suivantes : a. Renvoyer les résultats d'une requête silencieuse à l'organisme demandeur uniquement; b. Aucun avis ne doit être envoyé à d'autres organismes concernés, à l'exception de l'unité du GNCC; c. Les avis indiquant qu'il s'agit des mêmes critères de recherche sont également retenus par l'indicateur de requête silencieuse; d. Les requêtes silencieuses ne remplaceront pas les avis aux utilisateurs internes de la SNC. Elles ne s'appliqueront qu'aux avis aux organismes d'application de la loi et aux partenaires externes.	Maximum de 20 points (5 points par bonne réponse)		
CFC-4-27	**Correspondance sans accusé de réception** Le soumissionnaire devrait décrire comment la solution qu'il propose comprend une fonction de « correspondance sans accusé de réception » (voir le glossaire) où, selon l'étiquetage d'une entité de données, comme un élément dans la liste de surveillance, une occurrence n'est pas incluse dans les résultats d'une recherche, mais où la personne ou l'organisation à l'origine des données est avisée.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-28	**Recherche dans l'historique des requêtes** Le soumissionnaire devrait décrire comment la solution qu'il propose effectue une recherche dans un historique de requêtes afin de trouver des recherches similaires et fournit une réponse à indiquer : a. les critères similaires; b. la raison de la demande;	Maximum de 12 points (3 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	c. la date de la requête; d. l'organisme demandeur et l'utilisateur.			
CFC-4-29	**Recherche fédérée** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur d'effectuer une recherche fédérée dans tous les magasins de données de la SNC (p. ex. le catalogue de données, les magasins d'objets, les bases de données relationnelles) au moyen d'une seule requête.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-30	**Traitement des restrictions relatives aux résultats des requêtes** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'avoir des résultats de requêtes lorsque des restrictions de contrôle d'accès basé sur les rôles ou de contrôle d'accès basé sur les attributs interdisent la divulgation de renseignements, notamment : a. Possibilité d'indiquer que l'information existe et de fournir des coordonnées, sans pour autant divulguer les détails de l'information en tant que tels. b. Possibilité de ne renvoyer aucun résultat (selon les règles relatives à l'échange de données). c. Possibilité d'aviser le GNCC si aucun résultat ne peut être fourni.	Maximum de 12 points (4 points par bonne réponse)		
CFC-4-31	**Impression et enregistrement des résultats de recherche** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à l'utilisateur de gérer les résultats de recherche, ce qui comprend les fonctions suivantes : a. Impression; b. Enregistrement.	Maximum de 10 points (5 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
Conserver les règles administratives et les listes de surveillance				
CFC-4-32	**Gestion de la matrice de gravité** Le soumissionnaire devrait décrire comment la solution qu'il propose permet de créer et d'administrer les règles administratives configurables de la matrice de gravité que la solution utilisera pour calculer la note de gravité des soumissions et des demandes de services, notamment : a. Type de demande de services; b. Critères et règles de gravité applicables; c. Notes. La solution devrait permettre de créer et d'administrer des règles qui s'appliquent à de nombreux types de soumissions et de demandes de services, y compris les demandes de services et les soumissions d'organismes d'application de la loi, et les dossiers de plaintes du public du système national de signalement de la cybercriminalité et des fraudes.	Maximum de 15 points (5 points par bonne réponse)		
CFC-4-33	**Administration des règles administratives pour l'établissement des priorités** Le soumissionnaire devrait décrire comment la solution qu'il propose permettra de créer et d'administrer les règles administratives d'établissement des priorités utilisées pour mettre en évidence les soumissions qui sont susceptibles d'intéresser des sections particulières du GNCC, notamment : a. les règles propres à chaque section; b. les listes de surveillance propres à chaque section; c. les critères « d'intérêt » propres à chaque section; d. la capacité de configurer les règles en temps quasi réel.	Maximum de 20 points (5 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	Par exemple, la section du renseignement pourrait être intéressée par toute demande de rançon visant une municipalité de l'Ontario. Des règles administratives d'établissement des priorités peuvent être créées pour signaler à la section du renseignement les soumissions qui répondent à ce critère.			
CFC-4-34	**Administration des listes de surveillance** Le soumissionnaire devrait décrire comment la solution qu'il propose permettra à un utilisateur du GNCC de créer et de gérer des listes de surveillance pour différentes sections du GNCC. Les listes de surveillance devraient prendre en charge : a. des indicateurs de compromission spécifiques, comme des surnoms, des URL; b. des données plus complexes, comme des tactiques, des techniques et des procédures.	Maximum de 10 points (5 points par bonne réponse)		
CFC-4-35	**Configuration des règles administratives relatives à la logique de flux de travail** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC de gérer les règles administratives relatives aux flux de travail, notamment : a. capacité de créer et de modifier les règles qui dictent les flux de travail; b. capacité d'indiquer la date/les heures d'entrée en vigueur de la règle (début et fin); c. capacité de prendre en charge les modifications des règles sans qu'il y ait arrêt du système.	Maximum de 15 points (5 points par bonne réponse)		
Service de boîte à outils, de bac à sable et de base de connaissances				

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-4-36	**Administrer les demandes de boîte et leur utilisation** Le soumissionnaire devrait décrire comment la solution qu'il propose permet aux partenaires qui le demandent d'utiliser les applications et les services d'analyse médico-légale de cybercriminalité fournis par le GNCC, y compris : a. accorder l'accès aux outils; b. surveiller les activités de suivi liées à la configuration; c. surveiller l'utilisation des outils.	Maximum de 9 points (3 points par bonne réponse)		
CFC-4-37	**Utilisation des résultats des outils d'analyse médico-légale** Le soumissionnaire devrait décrire comment la solution qu'il propose est capable d'intégrer les résultats des outils d'analyse médico-légale dans le répertoire de la SNC aux fins de corrélation, de résolution d'incompatibilité et de connaissance de la situation, y compris comment la solution informera les utilisateurs du GNCC lorsque des corrélations sont établies en fonction des résultats de l'utilisation des outils.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-38	**Administration de la base de connaissances** Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'administrer le contenu de la base de connaissances mise à la disposition des utilisateurs du P3, y compris la manière dont du contenu peut être fourni par les partenaires du P3, examiné et modifié par le GNCC et publié dans la base de connaissances.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-39	**Administration du catalogue des services** Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur du GNCC d'administrer un catalogue des services du GNCC qui est accessible par l'intermédiaire du P3, notamment :	Maximum de 15 points (5 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	a. Créer et modifier les entrées, y compris les descriptions de services, les conditions préalables applicables, les notes d'utilisation et les critères de recherche; b. Gérer les dates de disponibilité des services (dates de début et de fin); c. Supprimer des entrées.			
Intelligence artificielle et apprentissage machine				
CFC-4-40	**Modèles d'apprentissage machine** Le soumissionnaire devrait décrire comment sa solution s'appuiera sur des modèles d'apprentissage machine et le traitement du langage naturel pour augmenter l'efficacité des processus du GNCC. Les modèles d'apprentissage machine et le traitement du langage naturel en question comprendront ce qui suit : a. triage et évaluation; b. analyse de données; c. flux de travail.	Maximum de 30 points (10 points par bonne réponse)		
CFC-4-41	**Normes de conformité en matière d'intelligence artificielle** Le soumissionnaire devrait décrire comment la solution qu'il propose aidera la GRC à se conformer aux principes directeurs en matière d'utilisation de l'intelligence artificielle et à la directive sur la prise de décision automatisée du Secrétariat du Conseil du Trésor. La solution sera évaluée en regard de l'évaluation de l'incidence algorithmique du Conseil du Trésor.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CFC-4-42	**Intelligence artificielle explicable**	Exigence démontrée : 10 points		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	Le soumissionnaire devrait décrire comment la solution qu'il propose garantit que les décisions prises à l'aide de l'intelligence artificielle sont explicables. Des méthodes explicables sont nécessaires (par opposition à une intelligence artificielle de type « boîte noire ») dans le cas où des décisions sont remises en question au cours de la procédure judiciaire.	Exigence non démontrée : 0 point		
CFC-4-43	**Utilisations de l'apprentissage machine** Le soumissionnaire devrait décrire comment la solution qu'il propose s'appuiera sur des modèles d'apprentissage machine pour répondre aux besoins opérationnels, ce qui comprend les besoins suivants : a. Repérage des signes avant-coureurs, c'est-à-dire des événements qui, lorsqu'ils sont remarqués, peuvent indiquer qu'une activité digne d'intérêt va suivre; b. Élaborer des profils de victimes, dans les cas où des groupes démographiques différents peuvent nécessiter un niveau de soutien et d'intervention différent de la part des organismes d'application de la loi; c. Élaborer des profils d'auteurs de menace dans le but d'identifier un individu qui représente une menace; d. Déterminer les déclencheurs et l'infrastructure criminelle, y compris les fournisseurs de services, les marchés de logiciels et de services du Web invisible, les intermédiaires; e. Élaborer des profils pour les dispositifs, les services, les lieux, et pour les auteurs de cybermenaces « non humains »; f. Permettre des simulations, y compris les tests d'hypothèses (que se passera-t-il si?); g. Caractériser les événements (p. ex. a-t-on déjà vu quelque chose qui se présente maintenant d'une manière différente?);	Maximum de 39 points (3 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	h. Permettre les activités de renseignement, y compris l'élaboration des flux d'activités, des flux de marchandises, l'analyse des schémas criminels, l'analyse financière et les profils de marché; i. Optimisation des requêtes; j. Optimisation de la saisie automatisée et de la réponse (conseils contextuels); k. Analyse sémantique; l. Classification du type de demande de services ou de soumission en fonction du contenu; m. Reconnaissance du ton (automutilation, violence, menaces).			
CFC-4-44	**Administration des modèles d'apprentissage machine** Le soumissionnaire devrait décrire comment la solution qu'il propose permet de faire en sorte que les modèles d'apprentissage machine soient : a. facilement codés; b. entraînés; c. mis à l'essai; d. optimisés (par exemple, l'optimisation des hyperparamètres); e. déployés en production; f. surveillés et administrés.	Maximum de 18 points (3 points par bonne réponse)		
CFC-4-45	**Suivi des modèles d'apprentissage machine** Le soumissionnaire devrait décrire comment la solution qu'il propose permet : a. de sauvegarder, de créer des versions et de récupérer les modèles d'apprentissage machine à partir de l'environnement de science des données; b. d'en faire le suivi au moyen d'indicateurs et de mesures de rendement après le déploiement en production.	Maximum de 10 points (5 points par bonne réponse)		
Traitement du langage naturel				

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CFC-4-46	**Utilisations du traitement du langage naturel** Le soumissionnaire devrait décrire comment la solution qu'il propose utilisera les capacités d'extraction de données des entités nommées du traitement du langage naturel et l'analyse de données pour déterminer les données qui sont utiles parmi les données non structurées (texte et images), y compris les données suivantes : a. Variables observables en matière de cybercriminalité et indicateurs de compromission; b. Incidents; c. Cibles; d. Tactiques, techniques et procédures adverses et défensives; e. Campagnes; f. Plans d'action; g. Auteurs de cybermenaces; h. Analyse du ton; i. Capacités multilingues.	Maximum de 27 points (3 points par bonne réponse)		
Renseignements organisationnels				
CFC-4-47	**Rapports d'aide à la décision** Le soumissionnaire devrait décrire comment la solution qu'il propose permettra de produire des rapports en temps réel et des rapports standards, personnalisés et spéciaux sur les sujets suivants : 1. Mesures opérationnelles : a. Nombre de requêtes effectuées par l'intermédiaire du P3; b. Nombre de demandes de référence croisée pour de logiciels malveillants; c. Présentations reçues; d. Demandes d'aide reçues et envoyées;	Maximum de 26 points. (2 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	e. Requêtes traitées; f. Corrélations trouvées; g. Dossiers de renseignements en cours ou achevés; h. Dossiers de coordination opérationnelle en cours ou achevés; i. Nombre de renvois de référence effectués ou classés; j. Partenariats établis; k. Mobilisation de partenaires privés. 2. Mesures stratégiques : a. Cybercrimes et fraudes par type, valeur, victime, lieu et autres attributs; b. Tendances, sur un mois et sur douze mois.			
CFC-4-48	**Exportation à Statistique Canada et à des partenaires** Le soumissionnaire devrait décrire comment la solution qu'il propose permettra d'exporter automatiquement des données sous forme de rapports standards et flexibles au Centre canadien de la statistique juridique de Statistique Canada et à d'autres partenaires externes.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Référence croisée de logiciels malveillants				
CFC-4-49	**Administration des demandes de référence croisée de logiciels malveillants** Le soumissionnaire devrait décrire comment la solution qu'il propose permettra d'administrer les demandes de référence croisée de logiciels malveillants des partenaires du P3, notamment les activités suivantes : 1. Réception des demandes de référence croisée de logiciels malveillants : a. Flux de travail d'admission et gestion de cas; b. Corrélation avec les bibliothèques de logiciels malveillants du GNCC (grâce à la comparaison de valeurs de hachage);	Maximum de 20 points 1.a. à 1.d., 2 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	c. Corrélation automatique et (s'il y a lieu) manuelle des indicateurs de compromission fournis avec la demande; d. Communication des résultats locaux ou demande d'envoi d'un échantillon par le P3; 2. Traitement des échantillons de logiciels malveillants : a. Échantillon de logiciel malveillant en quarantaine; b. Création d'une valeur de hachage et stockage dans la bibliothèque de logiciels malveillants du GNCC; c. Envoie d'un échantillon à des services externes d'analyse de logiciels malveillants aux fins d'analyse, tout en conservant une copie en quarantaine; d. Gestion des demandes en suspens; e. Réception, stockage, examen et communication des résultats des services d'analyse de logiciels malveillants; f. Production d'un rapport ou d'un bulletin d'analyse de logiciels malveillants en vue de sa publication dans la base de connaissances.	(2.a. à 2.f., 2 points par bonne réponse)		
Enrichissement automatisé				
CFC-4-50	**Résolution d'entités** Le soumissionnaire devrait décrire comment la solution qu'il propose rendra possibles la résolution d'entités et le repérage des liens entre les entités, ce qui comprend ce qui suit : a. Résolution d'incompatibilité et combinaison d'identités en ligne ou sur Internet fondées sur des attributs communs; b. Résolution automatisée d'entités des indicateurs de compromission; c. Examen manuel des entités résolues; d. Capacité de séparer les entités qui ont été résolues par erreur; e. Déclenchement automatique d'avis fondé sur des résolutions;	Maximum de 18 points (3 points par bonne réponse)		

Nº CFC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	f. Affichage et manipulation des entités au moyen d'un outil d'affichage des liens/réseaux.			
	Capacités fonctionnelles – Note totale ▶		**xx/824**	

5.4 CRITÈRES DE CAPACITÉS TECHNIQUES COTÉS

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
Capacités techniques				
Quarantaine des soumissions				
CTC-5-1	Le soumissionnaire devrait décrire comment la solution qu'il propose assurera la sécurité du GNCC tout en fournissant un maximum de renseignements sur les menaces à l'organisation grâce aux fonctions suivantes : a. Contrôle de toutes les soumissions, y compris le contenu chiffré, pour détecter le contenu malveillant; b. Arrêt du traitement si l'on trouve du contenu malveillant; c. Ingestion de soumission jugée propre; **d.** Mise à disposition des résultats de contrôle aux fins d'examen.	Maximum de 20 points (5 points par bonne réponse)		
CTC-5-2	Le soumissionnaire devrait décrire comment la solution qu'il propose traitera le contenu lié à l'exploitation, notamment : a. Recherche automatisée de contenu lié à l'exploitation b. Mise en quarantaine et traitement d'exception du contenu lié à l'exploitation c. Transmission de la soumission au Centre national de coordination contre l'exploitation des enfants (CNCEE) lorsque la soumission contient du contenu détecté lié à l'exploitation des enfants d. Si la solution n'a pas reconnu automatiquement le contenu lié à l'exploitation, permettre à un utilisateur du GNCC de transmettre le contenu lié à l'exploitation au CNCEE	Maximum de 20 points (5 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CTC-5-3	Le soumissionnaire devrait décrire comment la solution qu'il propose fournira à l'utilisateur un moyen d'examiner les soumissions qui ont été jugées contenant du contenu malveillant ou lié à l'exploitation, permettra de supprimer le contenu ou les pièces jointes malveillants ou liés à l'exploitation, et d'intégrer la soumission modifiée.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-4	Le soumissionnaire devrait décrire comment sa solution permet l'échange sécurisé d'information, y compris les courriels et les pièces jointes, en utilisant : a. la norme x.509; b. une norme de chiffrement de source ouverte par exemple, Pretty Good Privacy (PGP).	Maximum de 10 points (5 points par bonne réponse)		
Outils d'importation/exportation de données				
CTC-5-5	Le soumissionnaire devrait décrire comment la solution qu'il propose prendra en charge l'importation et l'exportation de données en utilisant des formats de fichier communs, y compris : a. l'importation de données d'un autre système en format XML et JSON; b. l'exportation de données vers un autre système en format XML et JSON; c. l'importation et l'exportation de données vers un outil d'analyse; d. l'importation et l'exportation de données à partir de sources ouvertes (par exemple, MISP); e. la création de constructions d'enregistrement utilisables comme des billets et des fichiers; f. l'importation et l'exportation de fichiers de données structurées, y compris des pièces jointes de données non structurées, entre les	Maximum de 30 points (5 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	partenaires du P3 et le Groupe national de coordination contre la cybercriminalité (GNCC).			
CTC-5-6	Le soumissionnaire devrait décrire comment la solution qu'il propose permettra d'échanger en toute sécurité des fichiers de plus d'un (1) téraoctet, notamment : a. Le transfert sécurisé de fichiers volumineux (fichiers de plus de 1 téraoctet); b. L'intégration transparente avec l'interface utilisateur de la SNC	Maximum de 20 points (10 points par bonne réponse)		
CTC-5-7	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la compression et la décompression de données en utilisant : a. ZIP b. LZH c. 7Zip d. GZIP e. WinRAR	Maximum de 10 points (2 points par bonne réponse)		
Normes d'échange de données				
CTC-5-8	Le soumissionnaire devrait décrire comment la solution qu'il propose permettra l'échange de données vers et depuis des systèmes externes en utilisant chacune des normes d'échange de données suivantes : a. STIX (Structured Threat Information eXpression) b. VERIS (Vocabulary for Event Recording and Incident Sharing) c. NIEM (National Information Exchange Model) d. TAXII (Trusted Advance eXchange of Indicators Information) e. LEIDS (Law Enforcement Information Data Standard)	Maximum de 12 points (2 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	f. Normes d'échange de données définissables par l'utilisateur qui peuvent être utilisées pour importer et exporter des données dans et hors de la solution			
Gestion de l'information				
CTC-5-9	Le soumissionnaire devrait décrire comment la solution qu'il propose soutiendra les capacités de gestion de l'information suivantes : a. Valider que les données reçues sont étiquetées avec les catégorisations de niveau de sécurité relatives à la communication et au traitement des données; b. Permettre à un utilisateur du GNCC de gérer les codes de catégorisation des données et de gérer les métadonnées relatives aux actifs de données du GNCC (p. ex. catalogage des données); c. Permettre à un utilisateur d'indiquer que le fichier contient un sujet de moins de 18 ans; d. Possibilité d'attribuer des catégorisations de niveau de sécurité et des codes de traitement aux données; e. Déclencher une alerte pour traitement d'exception si la désignation de sécurité d'une information dépasse la désignation du système Protégé B; f. Nouvel étiquetage, exportation et purge de l'information ayant dépassé le niveau de sécurité Protégé B.	Maximum de 18 points (3 points par bonne réponse)		
CTC-5-10	Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur de gérer la suppression physique des données comme suit : a. Supprimer du système les données inappropriées ou non autorisées; b. Exporter les données dans un fichier avant leur suppression physique.	Maximum de 10 points (5 points par bonne réponse)		
CTC-5-11	Le soumissionnaire devrait décrire comment la solution qu'il propose permet de réduire les coûts de stockage liés à la gestion des données :	Maximum de 15 points		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	a. Déplacement des données inactives ou archivées vers un stockage moins coûteux (p. ex. stockage de données à chaud ou à froid ou d'archivage); b. Récupération de données d'un stockage d'archives ou d'un stockage à froid en actif (stockage à chaud ou à froid); c. Fournir des paramètres de période configurables par l'utilisateur afin de définir automatiquement les périodes de conservation à chaud, à froid et d'archivage de différents types de données.	(5 points par bonne réponse)		
CTC-5-12	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge l'archivage et la purge (suppression logique), notamment : a. Purger l'information et les données à la fin d'une période de conservation définissable; b. Déterminer l'information et les données répondant aux critères d'archivage; c. Fournir un processus de confirmation de la purge des données pour permettre à un utilisateur d'approuver la purge des données et de modifier la date d'élimination si nécessaire; d. Prendre en compte les liens lors de la détermination des données à purger. Si un lien existe, les données liées sont soumises à la date de conservation la plus éloignée dans le futur; e. Paramètres de période configurables par l'utilisateur pour définir automatiquement les périodes d'archivage, de purge et de conservation de différents types d'enregistrements; f. Fonction de confirmation de la purge des données afin d'effacer ou de supprimer des données.	Maximum de 18 points (3 points par bonne réponse)		
CTC-5-13	Le soumissionnaire devrait décrire comment la solution qu'il propose peut être configurée pour intégrer des sources de données externes (p. ex. l'entrepôt de données d'entreprise ou un SGBD existant) dans une capacité d'interrogation fédérée de dépôt de la SNC, notamment :	Maximum de 15 points (5 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	a. Configurer et gérer les connexions aux magasins de données externes; b. Indexation dynamique d'un magasin de données externe; c. Incorporation de l'index dans une interrogation fédérée de dépôt de la SNC.			
Contrôle d'accès basé sur les rôles et les attributs				
CTC-5-14	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge le contrôle d'accès configurable basé sur les rôles et le contrôle d'accès configurable basé sur les attributs pour les fonctionnalités et l'information en fonction des rôles et des groupes d'utilisateur définissables. Le soumissionnaire devrait décrire comment la solution qu'il propose soutient le contrôle d'accès basé sur les rôles et le contrôle d'accès basé sur les attributs pour limiter l'accès en fonction de : a. Rôle d'utilisateur / de groupe; b. Emplacement de l'utilisateur; c. Sensibilité des données; d. Catégorisation du partage des données; e. Fonctionnalité (affichage, interrogation, ajout, mise à jour, suppression); f. Type de données (résultats d'interrogation, avis, fichiers, projets).	Maximum de 18 points (3 points par bonne réponse)		
CTC-5-15	Le soumissionnaire devrait décrire comment sa solution contrôle la divulgation d'information à l'aide de codes de communication de renseignements (par exemple, protocole des feux de circulation) et de désignations de sécurité des données pour ce qui suit : a. Avis; b. Messages; c. Résultats d'interrogation.	Maximum de 15 points (5 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
Intégration d'entreprise				
CTC-5-16	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge l'utilisation de normes ouvertes pour fournir des interfaces configurables (p. ex. JSON, API basée sur l'architecture REST, courtage de messagerie asynchrone) pour l'intégration de système avec les outils et composants suivants : a. Outils d'analyse des données; b. Outils de traitement du langage naturel; c. Outils d'extraction de texte; d. Outils géospatiaux (Esri); e. Outils de visualisation des données; f. Outils de conformité des données; g. Dépôts du domaine public sur la cybercriminalité; h. Outils de résolution d'entités; i. Outils de transcription et de traduction; j. Outils de reconnaissance optique de caractères; k. Outils d'analyse de réseau; l. Outils de gestion de cas; m. Outils de modélisation statistique; n. Outils d'aide à la décision / de rapports; o. Outils de recherche fédérée; p. Outils d'entrepôt d'entreprise.	Maximum de 32 points (2 points par bonne réponse)		
CTC-5-17	Le soumissionnaire devrait décrire comment la solution qu'il propose peut être configurée pour échanger des données avec des systèmes externes en utilisant des interfaces documentées mises en œuvre avec des API standard ouvertes de l'industrie qui : a. Utilisent les liaisons et les protocoles standard ouverts de l'industrie (y compris, mais sans s'y limiter, REST/JSON ou SOAP/XML);	Maximum de 15 points (3 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	b. Exposent les données sous forme de schémas d'entités commerciales ou d'objets non propriétaires; c. Respectent les normes du gouvernement du Canada sur les API telles que définies par : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html; d. Utilisent un bus de service ou un gestionnaire d'événements pour gérer les interactions de données entre les systèmes; e. Prennent en charge OpenAPI ou Swagger, pour faciliter la consommation et les essais.			
CTC-5-18	Le soumissionnaire devrait décrire comment la solution qu'il propose s'intégrera au système de messagerie électronique général de la GRC afin d'ingérer et d'envoyer des soumissions et des demandes de service.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Journal d'activités et de vérification				
CTC-5-19	Le soumissionnaire devrait décrire comment la solution qu'il propose consignera toutes les activités de l'utilisateur dans un journal d'activités immuable en lecture seule contenant : a. l'identifiant de l'utilisateur; b. l'horodatage de l'activité; c. l'activité réalisée; d. la valeur avant la modification des données; e. la valeur après la modification des données.	Maximum de 10 points (2 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CTC-5-20	Le soumissionnaire devrait décrire comment la solution qu'il propose permettrait à un utilisateur d'enregistrer une entrée manuelle dans le journal d'activités pour enregistrer des activités hors ligne telles que des appels téléphoniques ou des recherches dans des sources ouvertes.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-21	Le soumissionnaire doit décrire comment la solution qu'il propose consignera tous les accès des utilisateurs au système dans un journal de vérification immuable, notamment : a. qui s'est connecté; b. heure de connexion; c. heure de déconnexion; d. autorisations accordées; e. tentatives et échecs de connexion.	Maximum de 10 points (2 points par bonne réponse)		
CTC-5-22	Le soumissionnaire devrait décrire comment la solution qu'il propose conservera tous les critères de recherche d'interrogation et les résultats des interrogations subséquentes dans un journal d'interrogations immuable.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-23	Le soumissionnaire devrait décrire comment la solution qu'il propose tient à jour toutes les versions historiques d'un fichier si celui-ci est manipulé au cours de l'extraction de renseignements, de la traduction linguistique ou de toute autre activité d'analyse.	Exigence démontrée : 10 points		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
		Exigence non démontrée : 0 point		
CTC-5-24	Le soumissionnaire devrait décrire comment la solution qu'il propose consignera toutes les activités effectuées automatiquement par le système dans un journal de vérification immuable.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-25	Le soumissionnaire devrait décrire comment la solution qu'il propose offrira des capacités de recherche et d'affichage des journaux d'activités, de vérification et d'interrogations aux utilisateurs autorisés du GNCC, en fonction des autorisations configurables.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Clavardage textuel en ligne				
CTC-5-26	Le soumissionnaire devrait décrire comment la solution qu'il propose prendra en charge une fonction de clavardage/conférence en ligne sécurisée (Protégé B) comprenant ce qui suit : a. Ouvrir ou fermer un canal sécurisé pour lancer ou mettre fin à un clavardage; b. Inviter des utilisateurs à un clavardage; c. Permettre à des utilisateurs invités de se joindre à un clavardage; d. Surveiller les participants à un clavardage; e. Activer la voix; f. Activer la vidéo;	Maximum de 20 points (2 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	g. Activer les clavardages 1:1; h. Activer la messagerie; i. Saisir et enregistrer le contenu d'un clavardage entre les participants; j. Permettre l'échange de fichiers, y compris d'images.			
Publication de documents et applications de productivité				
CTC-5-27	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge l'intégration avec des outils de traitement de texte courants ou des liseuses/visionneuses appropriées aux fins : a. de l'accès, de la lecture, de la visualisation; b. de la modification; c. de la vérification orthographique de documents; d. de l'affichage de données structurées et non structurées; e. de l'affichage d'images dans le format de fichier natif.	Maximum de 10 points (2 points par bonne réponse)		
CTC-5-28	Le soumissionnaire devrait décrire comment la solution qu'il propose est capable de permettre à un utilisateur de créer et d'envoyer un courrier électronique (y compris un courrier électronique sécurisé) à un partenaire de lutte contre la cybercriminalité.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-29	Le soumissionnaire devrait décrire comment la solution qu'il propose offre la fonction « enregistrer sous » et la capacité de conversion de fichiers qui permettront de convertir un fichier d'un type à un autre, notamment : a. MS Word en PDF; b. MS Excel en PDF; c. Courrier électronique en PDF;	Maximum de 10 points (2 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	d. Image en PDF.			
CTC-5-30	Le soumissionnaire devrait décrire comment la solution qu'il propose offre aux utilisateurs internes autorisés du GNCC ou aux utilisateurs externes du P3 un environnement de collaboration sécurisé qui prend en charge l'accès, la modification, les commentaires et la discussion simultanés en temps réel des outils, des projets et des artefacts, y compris : a. Capacité à collaborer sur des documents texte, des feuilles de calcul, des PDF et des présentations; b. Capacité à collaborer sur des images ou des cartes de visualisation; b. Capacité à conserver l'historique et l'intégrité des révisions antérieures; c. Capacité d'un utilisateur à partager un écran pour afficher et démontrer des outils et des artefacts.	Maximum de 12 points (3 points par bonne réponse)		
Transcription, traduction et reconnaissance optique de caractères				
CTC-5-31	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la conversion audio/texte et la traduction linguistique, notamment : a. Lier les fichiers audio et textes initiaux et tous les fichiers texte résultants au fichier de la SNC connexe; b. Convertir et traduire l'audio (anglais et autres langues) en texte anglais; c. Traduire un texte anglais en texte français ou un texte français en texte anglais; d. Traduire un texte non anglais en texte anglais; e. Prendre en charge plusieurs langues autres que l'anglais ou le français; f. Indiquer le discours non natif dans le texte résultant; g. Déterminer les langues parlées dans un fichier audio;	Maximum de 16 points (2 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	h. Déterminer les différents orateurs dans un fichier audio.			
Gestion de l'identité				
CTC-5-32	Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur de gérer son mot de passe. La gestion du mot de passe doit être conforme aux normes de la GRC, notamment : a. Mot de passe obligatoire pour tous les utilisateurs; b. Le mot de passe contient un minimum de 8 caractères, dont un mélange de majuscules et de minuscules et au moins un caractère spécial; c. Le mot de passe doit être changé lors de la première connexion; d. Le mot de passe doit être changé au moins tous les six (6) mois; e. Les utilisateurs doivent pouvoir modifier leur mot de passe à tout moment; f. Les utilisateurs doivent être capables en tout temps de récupérer un mot de passe oublié; g. Processus de récupération du mot de passe oublié avec questions et réponses de l'utilisateur.	Maximum de 14 points (2 points par bonne réponse)		
CTC-5-33	Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur autorisé de la GRC de consulter, créer, modifier, suspendre ou rétablir un utilisateur de la solution provenant du GNCC ou du P3.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Facilité d'utilisation				
CTC-5-34	Le soumissionnaire devrait décrire comment la solution qu'il propose offre un rôle d'utilisateur admin ayant la capacité d'étendre et de personnaliser	Maximum de 14 points		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	les fonctionnalités de l'application en utilisant une approche à faible code ou sans code, notamment : a. tableaux de bord personnalisables; b. files d'attente de travaux personnalisables; c. listes de sélection de données configurables; d. ajout/configuration de règles administratives de validation; e. ajout/configuration de modèles de rapport; f. ajout/configuration de modèles et d'écrans de saisie d'entités de données et d'attributs de données; g. ajout/configuration de modèles de recherche.	(2 points par bonne réponse)		
CTC-5-35	Le soumissionnaire devrait décrire comment la solution qu'il propose permet la configuration sans entraîner de temps d'arrêt du système ou de nouvelles versions de logiciel.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-36	Le soumissionnaire devrait décrire comment la solution qu'il propose fournit une interface utilisateur dotée des éléments significatifs suivants : a. séquences de flux de travail; b. relations de l'information; c. accent sur des champs; d. messages; e. présentation uniforme; f. étiquettes d'écran; g. navigation et orientation cohérentes; h. avertissements aux utilisateurs.	Maximum de 16 points (2 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CTC-5-37	Le soumissionnaire devrait décrire comment la solution qu'il propose permet aux utilisateurs d'accéder à une aide en ligne contextuelle.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-38	Le soumissionnaire devrait décrire comment la solution qu'il propose facilite et normalise la saisie des données en faisant usage de : a. listes de sélection de données consultables; b. commandes de remplissage automatique; c. aide contextuelle / info-bulle; d. sélecteur de date et d'heure (widget de calendrier); e. indicateurs de progrès; f. commandes d'annulation.	Maximum de 12 points (2 points par bonne réponse)		
CTC-5-39	Le soumissionnaire devrait décrire comment la solution qu'il propose utilise au maximum les données existantes (p. ex. les données d'annuaire des clients ou des partenaires) afin de réduire au minimum la saisie de données par l'utilisateur (remplissage préalable et remplissage automatique) et de maximiser l'exactitude.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-40	Le soumissionnaire devrait décrire comment la solution qu'il propose permet à un utilisateur de créer une demande d'assistance.	Exigence démontrée : 10 points		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
		Exigence non démontrée : 0 point		
CTC-5-41	Le soumissionnaire devrait décrire comment la solution qu'il propose est disponible et accessible aux personnes handicapées, conformément aux normes d'accessibilité WCAG 2.0 A.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
Dépôt de la SNC				
CTC-5-42	Le soumissionnaire devrait décrire comment la solution qu'il propose est capable de stocker les données reçues dans plusieurs langues, telles qu'elles sont définies par les codes de langue ISO énumérés dans alpha-3/ISO 639-2.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-43	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge les normes sur les métadonnées, notamment : a. Norme sur les métadonnées du SCT du gouvernement du Canada (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18909); b. Ensemble d'éléments de métadonnées de Dublin Core (http://www.dublincore.org/); c. Prise en charge de la modification d'ensembles d'éléments de métadonnées.	Maximum de 9 points (3 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CTC-5-44	Le soumissionnaire devrait décrire comment la solution qu'il propose est capable de stocker, d'indexer et de faire des recherches à partir des formats de données suivants : a. Données structurées; b. Données semi-structurées; c. Données non structurées; d. Images; e. Vidéo.	Maximum de 10 points (2 points par bonne réponse)		
CTC-5-45	Le soumissionnaire devrait décrire comment la solution qu'il propose protège l'information et les données contre toute action et tout accès non autorisés.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-46	Le soumissionnaire devrait décrire comment la solution qu'il propose protège l'information et les données contre la perte et la corruption accidentelles ou délibérées.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-47	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge les capacités de stockage de données élastiques et évolutives.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
Surveillance de système				
CTC-5-48	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la surveillance de ce qui suit : a. Accès des utilisateurs (connexion, déconnexion); b. Croissance et utilisation des bases de données; c. Accès aux bases de données; d. Messages d'erreur; e. Tentatives répétées des utilisateurs; f. Utilisation des ressources infonuagiques (comme le calcul, le stockage, la messagerie); g. Trafic sur le réseau.	Maximum de 14 points (2 points par bonne réponse)		
CTC-5-49	Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'utiliser la capacité de collecte de journaux de l'espace infonuagique Protégé B de la GRC pour stocker et gérer tous les journaux, notamment : a. Journaux d'activités (événements du plan de contrôle relatifs aux ressources du gestionnaire de ressources); b. Journaux de ressources (données fréquentes sur le fonctionnement des ressources du gestionnaire de ressources relatives à un abonnement); c. Rapports Active Directory (journaux et rapports); d. Machines virtuelles et services en nuage (service de journal d'événements Windows et Syslog de Linux); e. Analyses du stockage (journalisation du stockage, fournit des mesures relatives à un compte de stockage); f. Groupe de sécurité de réseau (journaux de flux, format JSON, indique les flux sortants et entrants par règle); g. Aperçu d'applications (journaux, exceptions et diagnostics personnalisés);	Maximum de 16 points (2 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	h. Traitement des données / alertes de sécurité (alertes du centre de sécurité, alertes des journaux de surveillance).			
CTC-5-50	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge : a. l'avis de l'administrateur en cas de défaillance d'un composant du système; b. l'avis de l'administrateur en cas de tentatives répétées d'un utilisateur entraînant des messages d'erreur.	Maximum de 10 points (5 points par bonne réponse)		
Besoins non fonctionnels				
CTC-5-51	Le soumissionnaire devrait décrire comment la solution qu'il propose : a. saisit les exceptions d'exécution générées pendant le traitement des transactions opérationnelles de la SNC; b. traite les messages de file d'attente de lettre morte générés pendant le traitement des transactions opérationnelles de la SNC; c. documente le traitement des erreurs, y compris la récupération des erreurs; d. documente les politiques de répétition des tentatives; e. documente les politiques de compensation.	Maximum de 10 points (2 points par bonne réponse)		
CTC-5-52	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge l'analyse des erreurs en utilisant des identifiants de corrélation des messages pour faciliter le suivi et la journalisation des événements dans le système.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
CTC-5-53	Le soumissionnaire devrait décrire comment la solution qu'il propose permet aux administrateurs de système d'examiner les erreurs du système et de mettre à jour chaque erreur avec une résolution une fois qu'elle est résolue.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-54	Le soumissionnaire devrait décrire comment la solution qu'il propose fournit un client basé sur un navigateur comme interface utilisateur compatible avec : a. Internet Explorer v11 avec Windows; b. Google Chrome v80 et supérieure (avec Windows, MacOS, iOS, Android); c. Microsoft Edge v80 et supérieure (avec Windows, MacOS); d. Microsoft Edge v44 et supérieure avec iOS; e. Microsoft Edge v43 et supérieure avec Android; f. Firefox v74 et supérieure (avec Windows, MacOS); g. Firefox v23 et supérieure avec iOS; h. Firefox v67 et supérieure avec Android; i. Safari v12 et supérieure (avec macOS, iOS).	Maximum de 18 points (2 points par bonne réponse)		
CTC-5-55	Les soumissionnaires doivent décrire comment la solution qu'il propose prend en charge une conception réactive permettant de fournir un accès en utilisant n'importe quelle taille d'écran d'appareil, y compris un ordinateur de bureau, un ordinateur portable, une tablette ou un téléphone mobile : a. Fonction d'interrogation de la SNC;	Maximum de 20 points (5 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	b. Fonction d'avis; c. Fonction de demande de service; d. Fonction de soumission de données.			
CTC-5-56	Le soumissionnaire devrait décrire comment la solution qu'il propose offre ce qui suit : a. Une capacité d'identification unique qui permet aux utilisateurs internes d'accéder à toute la gamme des fonctionnalités autorisées; b. Une capacité d'identification unique qui permet aux partenaires externes d'accéder à toute la gamme des fonctionnalités autorisées.	Maximum de 10 points (5 points par bonne réponse)		
CTC-5-57	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge un délai d'expiration automatique après un temps d'inactivité configurable, après quoi une nouvelle authentification par l'utilisateur est nécessaire.	Exigence démontrée : 10 points Exigence non démontrée : 0 point		
CTC-5-58	Le soumissionnaire devrait décrire comment la solution qu'il propose étiquette automatiquement les données au fur et à mesure qu'elles sont ingérées, y compris : a. horodatage de réception; b. source du fournisseur de données; c. métadonnées de vérification; d. métadonnées de surveillance.	Maximum de 12 points (3 points par bonne réponse)		
CTC-5-59	Le soumissionnaire devrait décrire comment la solution qu'il propose saisit et conserve les métadonnées de lignage et de provenance des données tout au long des processus de transformation et d'intégration des	Exigence démontrée : 10 points		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	données, conformément aux normes sur les métadonnées du gouvernement du Canada. https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18909&section=html	Exigence non démontrée : 0 point		
CTC-5-60	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge ce qui suit : a. Validation des données; b. Contrôle de la qualité des données; c. Nettoyage des données pour les processus de saisie de données par lots; d. Nettoyage des données pour les processus de saisie de données en temps réel; e. Nettoyage des données pour les processus de saisie de données en temps quasi réel.	Maximum de 10 points (2 points par bonne réponse)		
CTC-5-61	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge la fédération de données en fournissant : a. accès virtuel aux bases de données structurées; b. accès virtuel aux données semi-structurées; c. la possibilité de réunir des données provenant de différentes sources pour un accès et une analyse en temps réel.	Maximum de 9 points (3 points par bonne réponse)		
CTC-5-62	Le soumissionnaire devrait décrire comment la solution qu'il propose prend en charge l'optimisation des interrogations : a. automatiquement dans le cadre des requêtes de SGBD; b. manuellement dans un éditeur SQL avancé.	Maximum de 6 points (3 points par bonne réponse)		
CTC-5-63	Le soumissionnaire devrait décrire comment les applications qu'il propose sont conçues et mises en paquet en se basant sur les meilleures pratiques relatives aux applications infonuagiques natives, notamment :	Maximum de 6 points		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	a. Conception et développement en tant qu'applications infonuagiques natives selon les méthodes d'applications à 12 facteurs; b. Utilisation de conteneurs d'un ou plusieurs micro-services avec des scripts paramétrés qui peuvent être adaptés à chaque environnement cible (p. ex. acceptation par l'utilisateur, contrôle de la qualité et production).	(3 points par bonne réponse)		
CTC-5-64	Le soumissionnaire devrait décrire comment la solution qu'il propose suit les meilleures pratiques dans la conception de ses scripts d'installation/de compilation, notamment : a. Scripts d'installation/de compilation dans un format lisible par code qui peuvent être déployés sous forme de paquet pour construire la solution dans l'environnement approprié; b. Scripts de mise à jour/correctif dans un format lisible par code et dans un format de paquet à déployer comme mise à jour d'application; c. Chaque composant devant être installé sur un serveur différent doit avoir son propre script de compilation dans un format lisible par code; d. Chaque version doit respecter la méthode de version et les exigences du dépôt de code de la GRC.	Maximum de 8 points (2 points par bonne réponse)		
Efficacité du rendement des services infonuagiques				
CTC-5-65	Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'obtenir et de maintenir un rendement efficace, notamment : a. Utiliser des déclencheurs automatisés pour surveiller le rendement du réseau afin de détecter les capacités inutilisées ou la dégradation, et adapter la solution en conséquence;	Maximum de 21 points (3 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	b. Utiliser des déclencheurs automatisés pour surveiller le rendement lié à la charge de travail des applications afin de détecter la capacité inutilisée ou la dégradation, et adapter la solution en conséquence; c. Utiliser des services gérés, pour réduire ou éliminer les frais administratifs et opérationnels généraux; d. Utiliser une approche basée sur les données, y compris des tests de charge périodiques pour faire évoluer la mise en œuvre de la solution afin d'atteindre un rendement efficient; e. Utiliser différentes solutions de calcul pour divers composants, au besoin, afin d'améliorer le rendement et d'utiliser les ressources de manière efficace; f. Utiliser plusieurs solutions et fonctionnalités de stockage, au besoin, afin d'améliorer le rendement et d'utiliser les ressources de manière efficace; g. Utiliser différentes solutions de bases de données pour divers sous-systèmes, au besoin, afin d'améliorer le rendement et d'utiliser les ressources de manière efficace.			
Efficacité des coûts liée au nuage				
CTC-5-66	Le soumissionnaire devrait décrire comment la solution qu'il propose permet d'obtenir et de maintenir une efficacité des coûts, notamment : a. Créer une structure de compte qui répartit clairement les coûts et l'utilisation entre les charges de travail des applications; b. Utiliser l'étiquetage des ressources pour appliquer les renseignements sur les entreprises et les organisations à l'utilisation et au coût;	Maximum de 21 points (3 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	c. Utiliser des tableaux de bord et des analyses personnalisés pour contrôler les coûts et l'utilisation à l'aide d'avis, de contrôles et de quotas de services; d. Surveiller l'utilisation des ressources pour détecter et corriger les zones de sous-utilisation importante, y compris la détection et l'arrêt automatique des ressources inutilisées; e. Utiliser des modèles d'établissement des prix à la demande ou réservés, au besoin, pour réduire au minimum les frais relatifs aux ressources; f. Utiliser un système de contrôle, un tampon ou une file d'attente pour niveler la demande et la servir avec moins de ressources, ce qui se traduit par un coût moindre; g. Utiliser un service de traitement en bloc pour traiter une charge de travail de manière asynchrone, à moindre coût.			
Activités infonuagiques				
CTC-5-67	Le soumissionnaire devrait décrire comment la solution qu'il propose recueille les informations nécessaires à partir des composants pour comprendre l'état de leur système interne et fournir des réponses efficaces le cas échéant, notamment : a. Mettre en œuvre le contrôle des modifications et la gestion des ressources du début du projet jusqu'à la fin de sa durée de vie; b. Définir, saisir et analyser les mesures de la charge de travail des applications afin d'avoir un meilleur aperçu des événements liés à la charge de travail, de manière à pouvoir prendre les mesures appropriées;	Maximum de 15 points (3 points par bonne réponse)		

Nº CTC	Description de l'exigence	Échelle de cotation	Note	Renvoi (Nº de page de la proposition)
	c. Définir, saisir et analyser les mesures DevOps afin d'avoir un meilleur aperçu des événements de déploiement et d'exploitation de manière à pouvoir prendre les mesures appropriées; d. Permettre la détection automatique des pannes de composants et des défauts de la charge de travail des applications, et le contournement automatique de ces événements lorsque cela est possible; e. Permettre une identification et une récupération rapides et automatiques des modifications de déploiement qui n'ont pas les résultats escomptés.			
Capacités techniques – Note totale ▶			**xx/867**	