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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
See Above

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet Cyberopérations défensives	
Solicitation No. - N° de l'invitation W6369-17DE25/B	**Date** 2017-12-18
Client Reference No. - N° de référence du client W6369-17DE25	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-049-26594
File No. - N° de dossier 049qe.W6369-17DE25	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-06-05**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (819) 420-1757 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See Herein	

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

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

Issuing Office - Bureau de distribution
Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Canada

PARTIE I - INTRODUCTION

Contexte

Le MDN et les FAC ont fortement investi dans des technologies qui ont radicalement augmenté la rapidité et la précision des opérations militaires modernes. La plupart de ces progrès incroyables en matière de capacité découlent de la dépendance à un cyberespace de plus en plus complexe. Pour s'acquitter de leurs principales responsabilités pour défendre le Canada, défendre l'Amérique du Nord et contribuer à la paix et à la sécurité internationales, le MDN et les FAC doivent être une force militaire moderne efficace, agile, adaptée, bien formée et bien équipée, dotée des capacités essentielles et de la souplesse qui sont requises pour faire face avec succès aux menaces conventionnelles et asymétriques, y compris les cyberattaques. Par conséquent, à l'appui de leur structure de commandement et de contrôle, le MDN et les FAC ont besoin de pouvoir surveiller et contrôler leur cyberespace afin qu'il reste défendable. À cette fin, deux des projets du programme de développement de la cyberforce du MDN et des FAC se concentrent sur l'application de ces exigences : sensibilisation à la cybersécurité (SC) et cyberopérations défensives - Aide à la décision (CD-AD) :

- Le projet en matière de SC transformera la façon dont le MDN et les FAC gèrent la confidentialité, l'intégrité et la disponibilité de leur cyberespace de plus en plus complexe. Cela se fera en se concentrant sur la détermination et la sécurisation de son cyberespace, en faisant preuve d'une connaissance intégrale de la situation qui permet aux commandants de prendre des décisions éclairées concernant la posture de sécurité de leur cyberespace.
- Le projet CD-AD améliorera la capacité du MDN et des FAC de mener des cyberopérations défensives (CD). Cela sera accompli en fournissant une capacité d'intervention contre les menaces sophistiquées et en améliorant la prise de décision des CD, rendant le processus plus souple, plus réactif et plus efficace afin de maintenir la liberté de manœuvre des commandants dans le cyberespace.

L'objectif est de créer une capacité de gestion de la cybersécurité défensive à la fine pointe de la technologie, composée du personnel du MDN et des FAC et des services professionnels, habilitée avec une gouvernance et une politique appropriées, et dotée des outils et des processus adéquats.

But de la présente DR

Services publics et Approvisionnement Canada (SPAC), au nom du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC), publie cette demande de renseignements (DR) pour informer l'industrie et pour obtenir des commentaires sur un éventuel processus d'acquisition pour les projets Cyberopérations défensives - Aide à la décision et sensibilisation à la cybersécurité (CD-AD et SC).

Comme ils sont étroitement liés, les deux projets ont été réunis dans une seule DR. Cette DR sera continuellement modifiée pour informer l'industrie sur une base continue des activités de consultation de l'industrie et de la rétroaction qui en résulte. Afin de faciliter le processus, le Canada a l'intention de maintenir la DR ouverte jusqu'au moment où une demande de propositions finale sera publiée. Toutefois, les réponses à la DR doivent être reçues au plus tard à la date indiquée dans le Tableau 1 – Activité d'approvisionnement ou de consultation et dates connexes.

Le processus de DR et d'engagement offre à l'industrie l'occasion de présenter ses capacités et ses points de vue concernant les exigences du Canada relativement au projet DCO-DS et CSA. Le Canada peut utiliser les informations recueillies pour l'élaboration d'une demande de propositions (DP). L'intention est de consulter activement l'industrie pendant tout le processus d'approvisionnement pour assurer une fin de projet réussie.

Parrainage en matière de sécurité : Étant donné que la DR comprend une annexe classifiée, et puisque la version préliminaire de la DP, la DP ainsi que le contrat subséquent peuvent contenir des renseignements classifiés, l'un des principaux objets de la présente DR consiste à fournir des directives et une assistance aux fournisseurs intéressés qui ne satisfont pas aux exigences de sécurité exposées en détail à l'annexe E afin qu'ils obtiennent l'attestation de sécurité requise. Veuillez consulter l'annexe I – Demande de parrainage en matière de sécurité pour obtenir des précisions sur le processus de parrainage. Les renseignements classifiés compris dans la DP subséquente, s'il y a lieu, ne seront fournis qu'aux fournisseurs qui satisfont aux exigences de sécurité.

Processus de consultation et d'approvisionnement proposé

Le processus de consultation et d'approvisionnement proposé pour les deux projets est expliqué en plus amples détails à la partie 1 de la présente DR et consiste en l'approche à plusieurs volets exposée ci-après. Veuillez noter que les activités d'approvisionnement qui ne sont pas comprises dans la portée de la DR initiale sont proposées aux fins de discussion seulement et peuvent être modifiées en tout temps. La décision d'exécuter d'autres activités d'approvisionnement n'a pas été prise.

Étape 1

Lettre d'intérêt : Une lettre d'intérêt (LI) réunissant les deux projets a été publiée en décembre 2016 sur le site Achatsetventes.gc.ca sous les invitations nº W6369-17DE25/A et W6369-17DE26/A. Elle a été fermée en janvier 2017. Au total, 31 entreprises ont répondu à la LI. Les résultats de la LI ont révélé qu'il était nécessaire de présenter une demande de renseignements (DR) plus détaillée.

Demande de renseignements : La présente DR vise à fournir des renseignements plus détaillés à l'industrie et servira de point permanent et unique pour les communications officielles sur le projet. Elle a surtout pour but de solliciter des commentaires détaillés de l'industrie sur les exigences opérationnelles et techniques, les coûts et le calendrier.

Journée de l'industrie non classifiée : Présenter un aperçu des exigences et du processus de consultation.

Rencontres individuelles : Les rencontres individuelles classifiées visent à distribuer et à présenter l'annexe classifiée de la DR, ainsi qu'à en discuter.

Réunion de suivi en groupe : Les réunions de suivi en groupe classifiées visent à distribuer les questions et réponses classifiées.

Étape 2

Demande de renseignements : La DR publiée à l'étape 1 demeurera ouverte afin de fournir des directives et une assistance aux fournisseurs pour qu'ils obtiennent l'attestation de sécurité requise.

Demande de propositions préliminaire : La version préliminaire d'une DP pour chaque projet ou un seul projet combiné peut être présentée aux fournisseurs qui satisfont aux exigences de sécurité aux fins d'examen et de commentaires.

Étape 3

Demande de propositions : La demande de propositions officielle pour chaque projet ou un seul projet combiné sera publiée.

Évaluation : Les soumissions seront évaluées conformément aux modalités de la DP.

Étape 4

Attribution du contrat : Le contrat sera attribué au soumissionnaire retenu conformément aux modalités de la

DP.

Calendrier d’approvisionnement

Le Canada en est à l’étape préliminaire d’un processus d’approvisionnement éventuel; il souhaite toutefois que les activités de consultation et d’approvisionnement soient réalisées selon le calendrier ci-dessous. Les fournisseurs doivent prendre note des dates limites de présentation des renseignements demandés par le Canada et les respecter.

Tableau 1 – Activité d’approvisionnement ou de consultation et dates connexes

Activité d’approvisionnement ou de consultation	Date
Parrainage d’attestation de sécurité*	De la date de publication de la DR à la date de publication de la DP
Étape 1	
Lettre d’intérêt	Terminé janvier 2017
Demande de renseignements (DR), inclus:	Maintenant jusqu'au l’automne 2019
Date limite pour s’inscrire à la réunion des représentants de l'industrie	février 16, 2018
Séance d'engagement des représentants de l'industrie non classé	février 26, 2018
Date limite pour s’inscrire aux rencontres individuelles classifiées	23 janvier, 2018
Rencontres individuelles classifiées	février 26, 2018 – mars 5, 2018
Date limite pour s’inscrire à la réunion de suivi en groupe	23 janvier, 2018
Réunion de suivi en groupe classifiée	À determiner – la semaine de mars 5, 2018
Répondre à la DR d'ici le	**Le 23 mars, 2018**
Étape 2	
Demande de propositions préliminaire	Automne 2019
Étape 3	
Demande de propositions	Été 2020
Évaluation	Automne 2020
Étape 4	
Attribution du contrat	Été 2021

*Les fournisseurs qui ne satisfont pas aux exigences de sécurité énoncées dans la DR, dans la DP et éventuellement dans le contrat seront parrainés afin qu’ils obtiennent l’attestation de sécurité requise par SPAC. Les fournisseurs ne répondant pas aux exigences de sécurité n’auront accès qu’à l’information destinée au public.

PARTIE II – DEMANDE DE RESEIGNEMENTS

1. CONSIGNES À SUIVRE POUR RÉPONDRE À LA PRÉSENTE DEMANDE DE RENSEIGNEMENTS

1.1. Nature et format des réponses demandées

On rappelle aux répondants que la présente est une DR et non une demande de propositions (DP). Ainsi, les répondants sont invités à fournir leurs commentaires, leurs préoccupations et leurs recommandations quant à la façon dont les exigences ou les objectifs décrits dans cette DR pourraient être satisfaits. Les répondants doivent expliquer les hypothèses qu'ils avancent dans leurs réponses.

Les réponses ne seront pas utilisées à des fins d'évaluation concurrentielle ou comparative et, par conséquent, le format des réponses n'est pas aussi rigoureusement défini qu'il le serait normalement pour une DP. Toutefois, dans le souci de recueillir des réponses qui seront faciles à traiter et qui auront la plus grande utilité, le Canada demande que les répondants suivent la structure décrite à la Format des réponses.

La participation ou la non-participation à la présente DR d'un fournisseur potentiel n'empêchera aucunement celui-ci de contribuer à un approvisionnement dans l'avenir. En outre, la présente DR n'entraînera pas nécessairement l'achat de l'un ou de l'autre des biens et des services qui y sont décrits.

1.2. Coûts des réponses

Le Canada ne remboursera aucune organisation pour les dépenses engagées afin de répondre à la présente DR, y compris, mais sans s'y limiter, les dépenses engagées pour participer à des activités d'engagement additionnelles

1.3. Traitement des réponses

Utilisation des réponses : Les réponses ne seront pas formellement évaluées. Toutefois, le Canada peut utiliser les réponses reçues pour élaborer ou modifier ses stratégies d'approvisionnement. Le Canada examinera toutes les réponses reçues. Cependant, s'il le juge opportun, il pourra examiner les réponses reçues après la date de demande de réponse à la DR.

Équipe d'examen : Une équipe d'examen composée de représentants du ministère de la Défense nationale et de Services publics et Approvisionnement Canada (SPAC) examinera les réponses. Le Canada se réserve le droit d'engager un consultant indépendant ou d'utiliser les ressources du gouvernement du Canada (GC) qu'il juge nécessaires pour l'examen des réponses. Tous les membres de l'équipe d'examen n'examineront pas nécessairement toutes les réponses.

Confidentialité : Les répondants doivent indiquer toute partie de leur réponse qu'ils considèrent comme exclusive ou confidentielle. *Loi sur l'accès à l'information* (L.R. 1985, ch. A-1), de la *Loi sur la protection des renseignements personnels* (L.R., 1985, ch. P-21) et de la *Loi sur la production de défense* (L.R. 1985, ch. D-1).

Précisions : S'il le juge à propos, le Canada peut communiquer avec les répondants pour leur poser des questions supplémentaires, obtenir des précisions sur un aspect d'une réponse ou encore pour effectuer des rencontres individuelles.

1.4. Exception au titre de la sécurité nationale

Afin de protéger les intérêts de sécurité nationale, le Canada invoque son droit prévu par les accords commerciaux nationaux et internationaux d'utiliser une exception au titre de la sécurité nationale (ESN) pour cette acquisition.

Une ESN permet au Canada de soustraire un approvisionnement à certaines ou à l'ensemble des modalités d'un accord commercial pertinent lorsqu'il le juge nécessaire afin de protéger sa sécurité nationale ou d'autres intérêts connexes précisés dans le texte des exceptions au titre de la sécurité nationale.

1.5. Nature et format des réponses demandées

Les répondants devront émettre leurs commentaires, faire part de leurs préoccupations et, le cas échéant, formuler des recommandations sur la façon de répondre aux exigences ou datteindre les objectifs décrits dans la présente DDR. Ils sont également invités à fournir leurs commentaires sur le contenu, la forme et la manière dont linformation est structurée dans les documents préliminaires joints à la présente DDR. Ils doivent sassurer dexpliquer toute hypothèse énoncée dans leurs réponses..

1.6. Contenu de la DR

Les renseignements contenus dans le présent document sont en cours d'élaboration. C'est pourquoi les répondants ne doivent pas perdre de vue que de nouvelles exigences pourraient être ajoutées à tout appel d'offres que publiera à terme le Canada. Il se peut également que des besoins soient retirés ou modifiés. Les répondants sont donc invités à faire part de leurs commentaires au sujet de tout aspect de la DR. Cette DR contient également des questions précises adressées à l'industrie.

1.7. Mise en garde relative aus invitations

La présente DR ne signifie pas que le Canada a pris une décision définitive quant aux possibilités d'approvisionnement. Le MDN et les FAC peuvent décider de ne choisir aucune des solutions ou aucun équipement identifiés dans les réponses. Le Canada ne sera en aucun cas tenu responsable envers un répondant qui fournit une réponse dans le cadre de la présente DR.

1.8. Format des réponses

L'industrie est invitée à répondre à cette DR et à fournir les informations suivantes au plus tard à la date de demande de réponse précisée. Les répondants sont invités à considérer ce qui suit dans la préparation de leur réponse :

Page couverture. Si la réponse comporte plusieurs documents, les répondants doivent indiquer sur la page couverture de chaque volume le titre de la réponse, le numéro de la demande, le numéro du volume et leur dénomination sociale complète.

Page titre. La première page après la page couverture doit être la page titre, qui doit contenir les informations suivantes :

1) le titre de la réponse du répondant et le numéro du volume;
2) le nom et l'adresse de répondant;
3) le nom, l'adresse et le numéro de téléphone de la personne-ressource du répondant;
4) la date;
5) le numéro d'invitation de la DR.

Mise en page et format de fichier. Le répondant peut utiliser la mise en page de son choix, mais il doit utiliser le modèle d'offres et d'évaluation des prix des produits fourni à l'annexe D et conserver la même numérotation pour faciliter l'examen et l'analyse de toutes les réponses par le Canada. Les réponses écrites doivent être fournies par

voie électronique en format MS Word, MS Excel ou PDF. La mise en page de la soumission doit suivre le format proposé ci-dessous :

6) Section 1 : Sommaire - 1 à 2 pages, résumant la soumission globale,
7) Section 2 : Profil de l'entreprise,
8) Section 3 : Concept de solution proposé,
9) Section 4 : Commentaires et conseils généraux;

Nombre de copies : Le Canada demande que les répondants présentent leur réponse dans un format non protégé (c'est-à-dire sans mot de passe) MS Word, MS Excel ou PDF par courrier électronique, si la taille du document est inférieure à 5 MB, à l'adresse suivante :

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Autrement, le Canada demande que les répondants enregistrent une copie de leur document PDF (2003 ou version plus récente) sur quatre clés USB et qu'ils les envoient à l'autorité contractante principale nommée ci-dessous.

1.9. Demande de renseignements

Toutes les demandes de renseignements et autres communications relatives à cette DR doivent être adressées exclusivement à l'autorité contractante de SPAC. Étant donné qu'il ne s'agit pas d'une invitation à soumissionner, le Canada ne répondra pas nécessairement par écrit et ne distribuera pas forcément les réponses aux répondants; néanmoins, les répondants qui ont des questions concernant la présente DR peuvent les transmettre à :

Autorité contractante primaire:
Patti Wight
Services publics et Approvisionnement Canada
Place du Portage III, 8C2
11 Rue Laurier, Gatineau, Quebec K1A 0S5
819-420-1757

Autorité contractante secondaire:
Jessica Strangemore
Services publics et Approvisionnement Canada
Place du Portage III, 8C2
11 Rue Laurier, Gatineau, Quebec K1A 0S5
819-420-1771

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Il est préférable de communiquer par courriel

Il est préférable de communiquer par courriel

Les fournisseurs sont invités à soumettre des questions et à formuler des commentaires mêmes s'ils ne participent pas à la journée de l'industrie ou aux rencontres individuelles.

Demandes de renseignements comportant des renseignements classifiés : Les fournisseurs **ne doivent transmettre aucune demande de renseignements par courriel** qui renferme des renseignements classifiés SECRET. Cela comprend les renvois aux précisions de l'annexe C. Les fournisseurs doivent simplement indiquer la page ou la ligne, entre autres, de l'annexe C à laquelle leur demande de renseignements se rapporte. Si la demande de renseignements doit comprendre des renseignements classifiés, les fournisseurs doivent communiquer avec l'autorité contractante de SPAC et attendre de recevoir ses directives, puisque les questions doivent lui être acheminées en personne.

1.10. Langue de la réponse

Les réponses peuvent être soumises en français ou en anglais, selon la préférence du répondant.

1.11. Présentation des réponses

Date et lieu de présentation des réponses : Le Canada demande que les fournisseurs soumettent leurs réponses au plus tard à la date de demande de réponse à la DR indiquée dans le tableau 1 – Activité d'approvisionnement ou de consultation et dates connexes. La date de clôture de la DR figurant à la page 1 de la DR n'est pas la date limite pour faire des commentaires. Les fournisseurs qui souhaitent présenter une réponse devraient la transmettre par courriel à l'autorité contractante susmentionnée avant l'heure et la date indiquées.

Réponses comportant des renseignements classifiés : Les fournisseurs ne doivent transmettre aucune réponse par courriel qui renferme des renseignements classifiés SECRET. Cela comprend les renvois aux précisions de l'annexe C. Les fournisseurs doivent simplement indiquer la page ou la ligne, entre autres, de l'annexe C à laquelle leur réponse se rapporte. Si la réponse doit comprendre des renseignements classifiés, les fournisseurs doivent communiquer avec l'autorité contractante de SPAC et attendre de recevoir ses directives, puisque la réponse doit lui être acheminée en personne.

Identification de la réponse : Chaque répondant doit s'assurer que son nom, son adresse et le numéro de la demande figurent lisiblement sur l'enveloppe contenant la réponse.

Retour de la réponse : Les réponses à la présente DR ne seront pas retournées.

Les commentaires seront acceptés jusqu'à ce que la demande de propositions soit publiée (le cas échéant).

1.12. Surveillance de l'équité

Le Canada a engagé les services d'une organisation à titre de tiers indépendant en vue d'agir comme surveillant de l'équité (SE). Le rôle du surveillant de l'équité est d'attester l'assurance de l'équité, de l'ouverture et de la transparence des activités surveillées.

Le surveillant de l'équité devra notamment assumer les responsabilités suivantes :

a. surveiller le processus d'approvisionnement en totalité ou en partie (ce qui comprend notamment les processus liés à l'engagement et à la DP prévue);
b. faire part au Canada de ses commentaires sur des questions relatives à l'équité;
c. attester l'équité du processus d'approvisionnement.

Veuillez noter que, dans le but d'exécuter ses obligations liées à la surveillance de l'équité, le surveillant de l'équité aura accès aux réponses de l'industrie et à la correspondance connexe reçue par le Canada à la suite de la présente DR. En outre, le surveillant de l'équité peut, à titre d'observateur, assister aux activités de suivi en matière d'engagement et de passation de contrats.

2. OBJECTIF DE LA PRÉSENTE DR

2.1. But

La présente DR est publiée avec les principaux objectifs suivants :

- Solliciter des prix indicatifs et des informations de planification pour l'acquisition et le soutien en service pour les exigences clés des projets SC et CD-AD.

- Solliciter des commentaires sur les capacités de l'industrie pour aider à l'élaboration de la proposition de valeur des RIT.
- Collaborer avec l'industrie au sujet des retombées industrielles et technologiques et de la stratégie de la proposition de valeur.
- Servir de point de contact permanent pour le Canada et l'industrie tout au long du processus de consultation et d'approvisionnement.
- Donner un aperçu de l'approche de consultation et du processus d'approvisionnement proposé.
- Fournir des mises à jour relatives au calendrier et à l'approvisionnement.
- Informer l'industrie des dates clés du processus de DR.
- Solliciter des commentaires détaillés de l'industrie sur le processus d'approvisionnement, les exigences opérationnelles et techniques, les coûts et le calendrier.
- Informer les fournisseurs des exigences de sécurité de la DR, de la DP préliminaire, de la DP et du contrat subséquent.
- Fournir des directives et de l'assistance aux fournisseurs qui n'ont pas d'attestation de sécurité pour qu'ils en obtiennent une.

2.2. Communication de renseignements classifiés (annexe C et questions et réponse classifiées)

Les répondants qui satisfont aux exigences de sécurité pour recevoir l'annexe C de la DR et assister aux rencontres individuelles, s'ils le demandent à l'autorité contractante :

a. seront invités à assister à une rencontre individuelle qui se déroulera dans un environnement classifié;
b. recevront l'annexe C à la rencontre individuelle;
c. seront invités à assister à une réunion de suivi en groupe afin de recevoir des copies papier des questions et réponses classifiées, s'il y a lieu.

L'annexe C sera remise en copie papier seulement et en personne au cours de la rencontre individuelle ou de la réunion de suivi en groupe. Elle ne sera pas remise en dehors de ces deux activités. L'annexe classifiée fournit des détails supplémentaires qui peuvent aider les fournisseurs à préparer leur réponse. Les fournisseurs doivent toutefois savoir que, bien que cette annexe présente les opérations en cours et les capacités en service au MDN de façon plus détaillée, elle n'est pas requise pour présenter une réponse exhaustive à la présente DR.

2.3 Licence concernant la propriété intellectuelle appartenant au Canada

L'industrie doit également savoir que le Canada a conçu un outil de défense automatisée des réseaux informatiques (ARMOUR) dans le cadre d'un projet de Recherche et développement pour la défense Canada (RDDC) et qu'il en détient la propriété intellectuelle (PI). Si un fournisseur souhaite faire des recherches sur cette PI, il doit en faire la demande par courriel à l'autorité contractante principale ou secondaire nommée à la section 1.9, qui la transmettra ensuite à RDDC. Veuillez noter que RDDC est entièrement responsable des demandes de renseignements et du processus d'octroi de permis se rapportant à cette PI.

3. SÉCURITÉ

La présente DR comporte des exigences relatives à la sécurité. Pour en savoir plus sur les enquêtes de sécurité réalisées sur le personnel et les entreprises, ainsi que sur les clauses de sécurité, les fournisseurs doivent consulter le site Web du Programme de sécurité des contrats (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html) de Travaux publics et Services gouvernementaux Canada.

L'un des principaux objectifs de la présente DR est d'informer les fournisseurs des exigences de sécurité obligatoires qui se rapportent aux diverses activités d'approvisionnement et de consultation, ainsi que de leur

permettre de demander d'être parrainés par SPAC pour qu'ils obtiennent leur attestation de sécurité et puissent ainsi participer au processus. Le Canada a l'intention de maintenir la présente DR ouverte jusqu'au moment où une DR finale sera publiée afin d'informer les fournisseurs des exigences de sécurité et de les aiguiller vers la Direction de la sécurité industrielle canadienne (DSIC) pour qu'ils puissent être parrainés et obtenir l'attestation de sécurité requise. SPAC cessera de parrainer les attestations de sécurité au moment où la DR finale sera publiée. Le Canada ne retardera pas la publication ou la clôture d'une DP afin de laisser aux fournisseurs le temps d'obtenir l'attestation de sécurité requise.

3.1 Exigences de sécurité applicables aux activités d'approvisionnement et de consultation

La DR, la version préliminaire de la DP, la DP et le contrat subséquent comprennent tous des exigences de sécurité obligatoires précises, tel qu'il est indiqué à la section 4.3 ci-dessous et à l'annexe E – Exigences relatives à la sécurité. Le tableau suivant, toutefois, est un résumé des exigences de sécurité par activité d'approvisionnement ou de consultation. Les attestations de sécurité doivent être délivrées par la Direction de la sécurité industrielle canadienne (DSIC) de SPAC. L'attestation de sécurité des fournisseurs étrangers sera confirmée par l'entremise de la Direction de la sécurité industrielle internationale (DSII), dans le cadre de ses propres programmes de sécurité industrielle intérieure.

Tableau 2 – Activité d'approvisionnement ou de consultation et exigences de sécurité connexes

Activité d'approvisionnement ou de consultation	Attestation de sécurité requise
Étape 1	
Demande de renseignements (DR) :	
Journée de l'industrie non classifiée	Aucune
Consulter l'annexe C	Attestation de sécurité d'installation : SECRET, CAN, ÉU, RU, AU Consultation de l'information par le personnel : SECRET, CAN, ÉU, RU, AU
Obtenir une version imprimée de l'annexe C Obtenir une version imprimée des questions et réponses classifiées, s'il y a lieu	Attestation de sécurité d'installation : SECRET, CAN, ÉU, RU, AU Membres du personnel qui transportent les documents : SECRET, CAN, ÉU, RU, AU Protection des documents : SECRET
Assister aux rencontres individuelles classifiées Assister à la séance de suivi en groupe classifiée	Attestation de sécurité d'installation : SECRET, CAN, ÉU, RU, AU Membres du personnel présents : SECRET, CAN, ÉU, RU, AU
Questions et réponses non classifiées	Aucune : elles seront accessibles au public
Étape 2	
Demande de propositions préliminaire*	Protection des documents : SECRET
Consulter l'information classifiée	Personnel : SECRET, réservé aux Canadiens
Obtenir une version imprimée de l'information classifiée	Attestation de sécurité d'installation : SECRET, réservé aux Canadiens Membres du personnel qui transportent les documents : SECRET, réservé aux Canadiens Protection des documents : SECRET
Assister aux rencontres classifiées	Personnel : SECRET, réservé aux Canadiens
Étape 3	
Demande de propositions*	Attestation de sécurité d'installation : SECRET, réservé aux Canadiens

	Personnel : SECRET, réservé aux Canadiens Protection des documents : SECRET
Consulter l'information classifiée	Personnel : SECRET, réservé aux Canadiens
Obtenir une version imprimée de l'information classifiée	Attestation de sécurité d'installation : SECRET, réservé aux Canadiens Membres du personnel qui transportent les documents : SECRET, réservé aux Canadiens Protection des documents : SECRET
Assister aux rencontres classifiées	Personnel : SECRET, réservé aux Canadiens
Étape 4	
Contrat*	Attestation de sécurité d'installation : TRÈS SECRET, réservé aux Canadiens Personnel : TRÈS SECRET SIGINT, réservé aux Canadiens* Protection des documents : SECRET, OTAN SECRET

*Il s'agit d'une version préliminaire pour le moment. Les exigences de sécurité peuvent modifiées tout au long du processus d'approvisionnement. Veuillez noter que les activités d'approvisionnement qui ne sont pas comprises dans la portée de la DR initiale sont proposées aux fins de discussion seulement et peuvent être modifiées en tout temps. La décision d'exécuter d'autres activités d'approvisionnement n'a pas été prise.

3.2 Parrainage d'attestation de sécurité pour les étapes 1 à 3

Les fournisseurs intéressés ou les soumissionnaires éventuels de l'industrie de la cybersécurité dont les organisations ne détiennent actuellement pas l'attestation requise pour les trois premières étapes du projet devraient entreprendre le processus d'obtention d'attestation de sécurité immédiatement. Le processus concernant les demandes de parrainage est décrit en détail à l'annexe J. Il incombe au fournisseur de s'assurer que l'information requise au sujet de l'attestation de sécurité est fournie à temps à l'autorité contractante ou à la DSIC.

Nous invitons fortement les fournisseurs à présenter rapidement leurs demandes d'attestation de sécurité. De plus, nous les encourageons vivement à soumettre des demandes d'attestation de sécurité pour leurs principaux employés qui pourraient avoir besoin d'accéder à des renseignements de nature délicate ou d'accéder à des sites sécurisés au cours de toute étape du projet, en commençant par l'engagement actuel de l'industrie jusqu'à l'attribution et l'exécution du contrat.

Des processus semblables, à quelques différences près, s'appliquent à tous les pays avec lesquels le Canada a des instruments de sécurité bilatéraux. Nous encourageons les fournisseurs étrangers à déterminer quelles sont les exigences dans leur pays visant les programmes de sécurité industrielle, afin de déterminer s'ils répondent à ces exigences et quelles sont les procédures précises qui s'appliquent dans leur pays. Comme susmentionné, il est fortement recommandé de s'inscrire le plus tôt possible.

Les activités de consultation et les approvisionnements subséquents, s'il y a lieu, ne seront pas retardés afin de laisser aux fournisseurs le temps d'obtenir les attestations de sécurité exigées.

3.3 Parrainage d'attestation de sécurité pour l'étape 4

Étant donné que les exigences de sécurité pour le contrat n'ont pas encore été établies définitivement, le Canada peut, ultérieurement, parrainer les fournisseurs intéressés ou les soumissionnaires éventuels de l'industrie de la cybersécurité dont les organisations ne détiennent actuellement pas les attestations prévues. Si le Canada choisit de parrainer les fournisseurs pour l'étape 4, la présente DR sera modifiée et ce processus y sera ajouté.

4. POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (RIT)

La Politique des retombées industrielles et technologiques (RIT) sera appliquée à ces projets. L'engagement de l'industrie dans le cadre de la demande de renseignements (DR) aidera à déterminer l'application de la Politique des RIT et la façon dont le Canada pourrait tirer profit des avantages économiques grâce à ce processus. Les fournisseurs peuvent consulter l'*ANNEXE F - Application de la Politique des retombées industrielles et technologiques (RIT)* pour un aperçu de la Politique des RIT et des questions à l'industrie relatives à cette exigence.

5. LANGUES OFFICIELLES

Tout marché éventuel pour une solution à ces projets exigera que l'entrepreneur fournisse tous les documents, le soutien technique et le soutien au client dans les deux langues officielles

6. APPROCHE EN MATIÈRE D'ENGAGEMENT

Le processus de consultation de l'industrie a commencé par une lettre d'intérêt et se terminera lorsqu'une demande de propositions finale sera publiée ou lorsque le Canada informera les fournisseurs que le processus de consultation est terminé. Comme les documents relatifs à l'invitation dans leur version définitive seront eux-mêmes classifiés, ils ne seront pas accessibles au public. Veuillez noter que l'approche en matière de consultation et les activités d'approvisionnement connexes qui ne sont pas comprises dans la portée de la DR initiale sont proposées aux fins de discussion seulement et peuvent être modifiées en tout temps. La décision d'exécuter d'autres activités d'approvisionnement n'a pas été prise.

Les fournisseurs qui souhaitent participer à l'une ou l'autre des activités de consultation, y compris la demande de l'annexe C, doivent examiner les règles d'engagement énoncées à l'annexe G.

Le Canada a l'intention d'employer l'approche progressive suivante pour le processus de consultation de l'industrie :

Activités de l'étape 1

Lettre d'intérêt : Une lettre d'intérêt (LI) initiale réunissant les deux projets a été publiée en décembre 2016 et sa date de clôture était en janvier 2017. La LI a permis d'informer l'industrie, à un haut niveau, des projets et a cherché à obtenir des commentaires généraux sur les solutions possibles et les coûts. Elle a avisé les fournisseurs potentiels que la Politique des RIT peut être appliquée. Au total, 31 entreprises ont répondu à la LI. Les résultats de la LI ont révélé qu'il était nécessaire de présenter une demande de renseignements (DR) plus détaillée.

Demande de renseignements : La présente DR fournit des renseignements plus détaillés à l'industrie et servira de point permanent et unique pour les communications officielles sur le projet. Les objectifs sont les suivants :

- Informer les fournisseurs des exigences de sécurité de la DR, de la DP et du contrat subséquent, et fournir des directives et une assistance aux fournisseurs qui n'ont pas d'attestation de sécurité pour qu'ils en obtiennent une.
- Solliciter des commentaires détaillés de l'industrie sur les exigences opérationnelles et techniques, les coûts et le calendrier.
- Demander des conseils sur les capacités de l'industrie à élaborer la proposition de valeur des RIT, à l'aide de questions au sujet de la capacité de l'industrie à exécuter les travaux liés aux contrats à venir au Canada, à renforcer les chaînes d'approvisionnement du Canada et à effectuer des investissements à long terme dans le secteur canadien de la cybersécurité.
- Répondre aux questions de l'industrie afin de veiller à ce que tous les participants intéressés reçoivent la même information. Les réponses classifiées seront distribuées en conséquence.

Journée de l'industrie non classifiée : Une journée de l'industrie non classifiée aura lieu dans la région de la capitale nationale, à Ottawa (Ontario). La journée de l'industrie à pour but de donner aux représentants inscrits de l'industrie un aperçu du processus de consultation, de l'approche en matière de consultation et des exigences de sécurité, ainsi qu'une vue d'ensemble non classifiée des projets. Cette journée vise à offrir une tribune où le Canada pourra faire connaître ses besoins à un haut niveau, et où l'industrie pourra poser des questions et recueillir de l'information afin de bien comprendre le besoin.

L'ordre du jour de la séance lors de la journée de l'industrie est le suivant :

1. Mot d'ouverture
2. Processus d'approvisionnement – Approche en matière de consultation
3. Exigences relatives à la sécurité
4. Aperçu du projet
5. Commentaires des fournisseurs et discussion sur les projets
6. Prochaines étapes et période de questions et réponses

Documents de la journée de l'industrie qui doivent être fournis aux participants :

a. Ordre du jour
b. Exemplaires des documents de présentation

Rencontres individuelles : Des représentants du Canada seront disponibles pour tenir des rencontres individuelles avec les fournisseurs inscrits, qui satisfont aux exigences de sécurité décrites à l'annexe E. Ces rencontres seront classifiées et auront lieu dans une installation sécurisée du MDN.

Objectifs de la rencontre :

1. Remettre aux fournisseurs une version imprimée de l'annexe C. Celle-ci sera remise en personne seulement.
2. Donner aux fournisseurs un aperçu de l'annexe C classifiée.
3. Inviter les fournisseurs à faire part de leurs commentaires et à discuter de l'annexe C seulement.

Les fournisseurs qui satisfont aux exigences de sécurité et qui souhaitent prendre part à une consultation individuelle auprès des fournisseurs doivent en faire la demande et s'inscrire, conformément à l'annexe I. Les fournisseurs qui demandent une rencontre avec les représentants du Canada recevront des renseignements supplémentaires et devront déterminer les dates qui leur conviennent dans une période précisée. Le Canada leur confirmera alors l'une des dates demandées ou encore lui en suggérera une autre. Les dates des rencontres seront attribuées suivant le principe du « premier arrivé, premier servi ».

Toutes les consultations individuelles auprès des fournisseurs et la réunion de suivi en groupe seront terminées avant la date de demande de réponse à la DR. Le Canada peut demander des consultations individuelles avec les fournisseurs en tout temps pendant ou après la date de demande de réponse à la DR pour obtenir des précisions sur les commentaires reçus.

Réunion de suivi en groupe : Afin de distribuer les questions et réponses classifiées aux fournisseurs qui satisfont aux exigences de sécurité décrites à l'annexe E, une seule réunion de suivi en groupe aura lieu dans une installation sécurisée du MDN. À l'occasion de cette réunion, une version imprimée des questions et réponses issues des rencontres individuelles sera distribuée aux fournisseurs qui satisfont aux exigences de sécurité. Aucune

discussion ne sera tenue à cette réunion. Les fournisseurs qui satisfont aux exigences de sécurité et qui ne se sont pas présentés à une rencontre individuelle peuvent très bien assister à la réunion de suivi en groupe pour obtenir un exemplaire de l'annexe C et des questions et réponses classifiées, s'il y a lieu.

Activités de l'étape 2

Demande de renseignements : La DR publiée à l'étape 1 demeurera ouverte, et les activités suivantes se poursuivront :

- Informer les fournisseurs des exigences de sécurité de la DR, de la DP et du contrat subséquent éventuel, et fournir des directives et une assistance aux fournisseurs qui n'ont pas d'attestation de sécurité pour qu'ils en obtiennent une.
- Répondre aux questions de l'industrie afin de veiller à ce que tous les participants intéressés reçoivent la même information. Ces activités continueront d'être exécutées conformément aux exigences de sécurité liées à l'annexe C.

Demande de propositions préliminaire : Une DP préliminaire pour chaque projet ou un seul projet combiné sera distribuée à l'industrie afin de préciser davantage le besoin en abordant les préoccupations de l'industrie et en tenant compte de ses recommandations. Seuls les fournisseurs qui satisfont aux exigences de sécurité décrites à l'annexe E auront accès aux volets classifiés de la DP préliminaire.

Activités de l'étape 3

Demande de propositions : La version définitive de la demande de propositions pour chaque projet ou un seul projet combiné sera distribuée à l'industrie. Un processus normal de questions et de réponses sera suivi. La consultation active de l'industrie au cours du processus de consultation rapide devrait permettre de réduire le nombre de questions et de préoccupations.

Évaluation : Les soumissions seront évaluées conformément aux modalités de la DP.

Activités de l'étape 4

Attribution du contrat : Le contrat sera attribué au soumissionnaire retenu conformément aux modalités de la DP.

7. DEMANDES DE RENSEIGNEMENTS PAR LE CANADA

7.1. Documents d'intérêt

Les documents suivants, pour lesquels le Canada cherche à obtenir des commentaires de l'industrie, sont joints à la présente DR :

- Annexe A - Contexte du projet;
- Annexe B - Énoncé des besoins opérationnels préliminaire;
- Annexe C - Concept d'opération actuel et capacités en service (CLASSIFIÉ);
- Annexe F - Application de la Politique des retombées industrielles et technologiques (RIT).

Les renseignements contenus dans ces documents en sont à l'étape préliminaire et sont toujours en cours d'élaboration. C'est pourquoi les répondants ne doivent pas perdre de vue que de nouvelles exigences pourraient être ajoutées à tout appel d'offres que publiera éventuellement le Canada. Il se peut également que des exigences soient retirées ou modifiées. Ils sont toutefois invités à formuler des commentaires sur n'importe quel élément des documents provisoires.

7.2 Document d'orientation et d'inscription

Les annexes suivantes fournissent des conseils additionnels sur la façon de répondre à la présente DR, les règles relatives à l'engagement et le processus d'inscription pour les réunions et les demandes d'informations classifiées :

- Annexe D – Modèle d'offres et d'évaluation des prix des produits;
- Annexe E – Security Requirements;
- Annexe G – Règles d'engagement;
- Annexe H – Inscription pour assister à la réunion des représentants de l'industrie;
- Annexe I – Registration for One-on-One Meetings, Group Follow-up Meeting; and
- Annexe J – Request for Security Sponsorship.

7.3 Invitation à répondre

Tous les répondants intéressés, peu importe qu'ils satisfassent aux exigences de sécurité, sont invités à fournir une soumission écrite qui comprend notamment ce qui suit :

a. une description des solutions et des produits proposés couvrant l'ensemble ou certains des composants fonctionnels théoriques décrits à l'annexe B dans la vision architecturale des composants théoriques;
b. les prix indicatifs, la structure de répartition du travail et la planification des produits et solutions proposés, y compris les tâches d'intégration, d'installation, de configuration, de mise à l'essai et de formation liées à ces derniers;
c. les prix indicatifs et le calendrier du soutien en service et des tâches d'entretien continu;
d. l'approche d'approvisionnement proposée avec des recommandations pour l'approvisionnement concurrentiel, les critères de sélection et la base de paiement;
e. des recommandations ou conseils supplémentaires concernant les exigences et les plans du projet.

7.4 Demande de renseignements

En utilisant le format identifié à la section 1.8, le Canada demande des réponses comme suit :

Section 1 – Sommaire: 1 à 2 pages résumant la soumission globale du répondant;

Section 2 - Profil de l'entreprise:

1) Fournir une brève présentation et la description de la capacité de l'entreprise, mettant en relief les produits, les services, les capacités basées au Canada et l'expérience dans la fourniture de solutions pertinentes aux objectifs du projet,

2) Décrire l'intention et la capacité de remplir le rôle d'intégrateur de système principal, de sous-traitant potentiel ou de fournisseur de produits ou de services dans le cadre d'un des projets ou des deux projets, ou pour tout élément ou partie spécifique de la présente DR;

3) Décrire les partenariats établis avec d'autres industries, le cas échéant, qui seraient profitables pour le développement des exigences de capacité du projet;

4) Décrire le rôle ou l'approche de la Politique des retombées industrielles et technologiques (RIT) présentée à l'annexe E;

5) Décrire les principales hypothèses, contraintes, préoccupations, conclusions et recommandations que, selon le répondant, le Canada devrait considérer afin que le projet évalue les différentes options;

Section 3 - Concept de solution proposé. Les répondants sont priés de fournir ce qui suit :

1) **Aperçu du plan de solution :** un aperçu du concept, de la structure de répartition du travail de haut niveau et d'un calendrier pour un produit livrable ou tous les produits livrables définis à l'annexe B que le répondant a l'intention de fournir, décrivant les principaux produits et composants, les logiciels, le matériel et les services techniques. Les fournisseurs doivent, dans le contexte de l'information figurant à l'annexe B, faire ce qui suit :

   i. fournir une description de la façon dont les caractéristiques et les capacités proposées de leur système respectent ou dépassent les exigences énoncées à l'annexe B (noter que les fournisseurs peuvent proposer des solutions qui ne sont pas nécessairement conformes aux composants fonctionnels décrits à l'annexe B dans la vue architecturale conceptuelle, à condition que l'ensemble de la solution réponde aux exigences);

   ii. fournir leur approche pour maintenir l'intégrité des données, des produits, des sous-systèmes et du système dans un environnement contesté;

   iii. fournir leur approche en matière d'innovation en vue de maintenir la pertinence des capacités tout au long du cycle de vie. Décrire comment la solution proposée atteint les qualités opérationnelles souhaitées déterminées à l'annexe B;

   iv. indiquer le degré de modularité déployable de leur solution et ses composants,

   v. fournir leur approche pour ingérer et intégrer les flux de données existantes, fondée sur des modèles de données et une expérience antérieure dans ce domaine, selon le cas;

   vi. indiquer le caractère évolutif de leurs solutions pour répondre aux besoins plus importants de l'entreprise, allant jusqu'à plus de 150 000 utilisateurs du réseau, 125 000 points d'extrémité (bureau et VHD), 6 000 serveurs et jusqu'à 150 cyberopérateurs ayant simultanément accès au système.

   vii. fournir des détails sur le déploiement de la solution, y compris les approches progressives pour l'élaboration, les mises à l'essai, la mise en œuvre, la formation et les mises à niveau;

   viii. fournir une fiabilité et une disponibilité du produit, du sous-système et du système à partir des données historiques;

   ix. indiquer les risques d'ordre technique et liés à la gestion, à la formation, à la sécurité, au soutien et au calendrier, ainsi que les mesures d'atténuation qu'ils recommandent. Si un risque peut être atténué en modifiant les politiques existantes, les CONOPS ou l'architecture, le fournisseur doit se sentir libre de recommander une telle stratégie d'atténuation.

2) **Plan détaillé de haut niveau et séquence d'événements :** un plan et un calendrier indicatifs du projet (mesuré en mois après l'attribution du contrat) pour la livraison de tout produit ou de tous les produits livrables définis à l'annexe B que le répondant a l'intention de fournir. Pour les réponses des intégrateurs de systèmes, dans le but de calculer avec précision le coût des deux projets, des plans distincts pour le projet de SC et le projet de CD-AD sont exigés mais, le cas échéant, l'identification et les commentaires à l'effet de toute économie potentielle résultant de la mise en œuvre des deux projets en tant qu'initiative unique peut également être soumise,

3) **Coûts estimés pour chaque livrable:** une estimation de coût indicative, avec une description par unité, pour tout produit ou tous les produits livrables définis à l'annexe B que le répondant a l'intention de fournir. L'objectif est d'estimer en toute confiance le coût total de possession sur la durée de vie de la capacité. Pour ce faire, le fournisseur doit présenter une aperçu afin que les coûts de développement, de mise à l'essai, de déploiement, de soutien et de mise à niveau, y compris les coûts récurrents et non récurrents, soient clairement identifiés et répartis pour l'ensemble du cycle de vie. Des informations additionnelles sur les coûts du soutien sont souhaitables. Il est reconnu que les modèles de tarification des fournisseurs varient en fonction du nombre d'événements par seconde, du nombre de dispositifs de point d'extrémité déployés, de l'utilisateur ou des abonnements à honoraires fixes, entre autres. En complétant le modèle de données sur les coûts fourni à l'annexe D, les répondants sont invités à indiquer clairement comment chaque produit livrable est fourni avec ses coûts annuels estimés de soutien en service. Par exemple, si la livraison d'une capacité nécessite des unités matérielles et logicielles discrètes, du personnel de soutien ou du personnel du centre d'opérations, les fournisseurs doivent clairement l'indiquer dans la base de coûts unitaires, le prix par unité ou le nombre d'unités requis. À tout le moins, la réponse doit indiquer que le coût de la solution se calcule facilement à l'aide du modèle simple suivant :

Coût = prix / unité x nombre d'unités

Section 4 : Commentaires et conseils généraux. Les répondants sont invités à fournir des commentaires, des remarques et des conseils concernant ce qui suit :

1) les objectifs de rendement, les exigences opérationnelles ou les composants fonctionnels théoriques décrits à l'annexe B;

2) les capacités actuelles décrites à l'annexe C, y compris les structures organisationnelles des unités opérationnelles;

3) les matrices de conformité des données d'attributs des entités cybernétiques pour les entités cybernétiques humaines et non humaines fournies dans les appendices de l'annexe D;

4) les questions des RIT et de PV qui sont fournies à l'annexe E;

5) l'amélioration des descriptions de projets, des objectifs, de la gestion et des approches d'approvisionnement pour améliorer l'efficacité globale de la mise en œuvre;

6) Solutions proposées;

   i. Que la solution proposée soit pour SC, CD-AD ou les deux? La solution proposée répond-elle à toutes les exigences de la solution sélectionnée (SC / CD-AD)?

   ii. Énumérer les composants tiers (fournisseurs) commercialement disponibles et / ou open source nécessaires pour s'intégrer à la solution proposée pour la compléter?

   iii. Comment la solution proposée, y compris les composants tiers commercialement disponibles et / ou open source sélectionnés, intègrent-ils et inter opèrent-ils dans un environnement technologique diversifié? La solution proposée est-elle destinée à réutiliser et à intégrer les composants existants du MDN / FAC?

iv. Comment la solution proposée intègre-t-elle des données et distribue-t-elle des données à plusieurs niveaux de sécurité et restrictions?

v. Les composants de la solution proposée seront-ils rendus inefficaces dans un environnement déconnecté, intermittent et à faible bande passante et dans quelle mesure les interruptions peuvent-elles être récupérées? Quelles sont les alternatives proposées à apporter dans un environnement déconnecté, intermittent et faible bande passante et les coûts associés à cela?

vi. Comment la solution proposée suivrait-elle tous les détails liés aux cyber-entités non-humaines connectées au réseau (autorisées et non autorisées), leur état logique et physique et leur emplacement?

vii. La solution proposée offre-t-elle une personnalisation et une extensibilité via une interface de script ou de programmation?

viii. Quelle est la solution de stockage de données proposée pour l'entreprise?

ix. Le MDN / FAC pourrait-il obtenir une licence de démonstration des composants de solution proposés pour son environnement de test et d'évaluation?

7) Informations sur les menaces :

i. Quelles sources et formats d'informations sur les menaces seraient intégrés?

ii. Comment les sources de la menace peuvent-elles être échangées / partagées avec les partenaires de la mission et les alliés?

8) Security Intégrité et sécurité de la chaîne d'approvisionnement

i. Les références:

a) https://www.cse-cst.gc.ca/fr/page/conseils-chaine-dapprovisionnement-technologies

b) https://www.cse-cst.gc.ca/fr/node/300/html/25733

c) https://www.cse-cst.gc.ca/fr/node/299/html/25729

ii. Le Centre de la sécurité des télécommunications Canada (CSTC) offre des conseils et de l'orientation en matière de sécurité des TI au GC quant aux menaces et vulnérabilités associées à la chaîne d'approvisionnement, ainsi que des conseils en matière d'atténuation et de prévention.

iii. Le guide Clauses contractuelles liées à l'équipement et aux services de télécommunication (TSCG-01\G) fournit des clauses de sécurité à intégrer dans les contrats de Travaux publics et des Services gouvernementaux Canada (TPSGC) en vue de prévenir ou d'atténuer les risques liés à la chaîne d'approvisionnement concernant les réseaux de communication et l'infrastructure de technologie de l'information (TI) du GC, souvent appelé Intégrité de la chaîne d'approvisionnement.

iv. Les clauses sont fondées sur des scénarios de services de télécommunication gérés, où un entrepreneur est responsable de sélectionner, de déployer, d'exploiter et d'entretenir les services et l'infrastructure de télécommunication destinés aux clients GC. Certaines clauses sont également utiles

pour l'approvisionnement d'équipement ou des solutions TI. Les lignes directrices présentent un processus de sélection et d'adaptation de clauses données, y compris celles qui touchent le coût, l'échéancier et les exigences.

v. La fiche d'information Clauses contractuelles liées à l'équipement et aux services de télécommunication (TSCG-01\L) décrit l'objectif visé et donne un aperçu des catégories de clauses.

vi. Question: Comment ces clauses contractuelles pourraient-elles affecter le coût, le calendrier et la conception de votre solution proposée? De quelles informations supplémentaires votre entreprise at-elle besoin pour mieux répondre aux coûts, planifier et concevoir les risques imposés par les restrictions liées à l'intégrité de la chaîne d'approvisionnement?

9) tout autre sujet de préoccupation ou conseil qui aiderait à fournir une recommandation d'amélioration pour la définition des projets et leur mise en œuvre.

ANNEXE A:CONTEXTE DU PROJET

ANNEXE A : CONTEXTE DU PROJET

1 Introduction

1.1 État du projet

Les exigences de capacité sont présentées sous la forme de deux projets distincts mais liés : Sensibilisation à la cybersécurité[1] (SC) et Cyberopérations défensives - Aide à la décision (CD-AD). Les deux projets sont actuellement dans la phase d'analyse des options[2] dans le but de présenter l'approche privilégiée du Conseil du Trésor (CT) du Canada au printemps de 2019. Pour recevoir l'approbation de passer à la phase de définition[3] pour les projets, il est **essentiel** que les coûts indicatifs[4] et les calendriers soient déterminés pour la mise en œuvre des projets. Des commentaires de l'industrie sont donc sollicités en ce qui concerne les modèles de coûts et les devis pour les services professionnels, la technologie, le matériel, les logiciels, le soutien de la gestion de projet et les travaux d'intégration et de durabilité qui sont nécessaires pour satisfaire les besoins de l'entreprise et les exigences quant à ces deux projets.

1.2 Besoin opérationnel

Afin de répondre aux besoins opérationnels d'un cyberespace contesté et de maintenir l'efficacité de l'entreprise et l'efficacité opérationnelle en tant qu'organisation responsable de la sécurité au sein du gouvernement du Canada (GC), les commandants, les cadres, les gestionnaires et les opérateurs du MDN et des FAC ont besoin d'une capacité de maintien de la cybersécurité et de la connaissance de la situation (l'objectif du projet de SC), intégrée avec une capacité pour réaliser une analyse contextuelle approfondie pour soutenir leurs décisions et leurs actions au moyen des cyberopérations défensives (CD) (l'objectif du projet CD-AD).

Le projet de SC vise à fournir une connaissance intégrale de l'emplacement (logique et physique), du statut et de la configuration du cyberespace du MDN et des FAC. Cette sensibilisation accrue améliorera la responsabilisation des entités du cyberespace du MDN et des FAC et améliorera la posture de sécurité dudit cyberespace, ce qui

---

1 La **cybersécurité** est définie comme l'« ensemble de technologies, des processus, des pratiques et des mesures d'atténuation et d'intervention conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés afin d'assurer la confidentialité, l'intégrité et la disponibilité », TERMIUM Plus [MD], la banque de données terminologiques et linguistiques du gouvernement du Canada, 9 octobre 2014.

2 La **phase d'analyse des options** est la deuxième étape du processus d'approbation du projet utilisé par le MDN et les FAC. Un livrable clé de cette phase est une estimation des coûts indicatifs (normalement établie par des demandes de renseignements et des demandes de prix et de disponibilité de l'industrie) du budget qui sera nécessaire pour mettre en œuvre la solution du projet.

3 La **phase de définition** est la troisième étape du processus d'approbation du projet utilisé par le MDN et les FAC. Une livraison clé de cette phase est une estimation des coûts *fondée* (normalement établie par une demande de propositions officielle de l'industrie) du budget qui sera nécessaire pour mettre en œuvre la solution du projet.

4 Les **coûts indicatifs** sont une estimation des coûts reposant sur les coûts normalisés et la recherche. Le niveau de détail engloberait la granularité des dépenses prévues pour tous les coûts représentant plus de 10 % de la valeur du contrat et pour lesquels de nombreuses soumissions ont été reçues de la part de fournisseurs éventuels, l'identification des composants et des plans pour les postes par rang *[aptitudes/expertise requises]*. Le prix réel du contrat se situera à +/- 25 % de la valeur indicative. Guide d'établissement des coûts du MDN, deuxième édition - avril 2006.

permettra des réponses appropriées aux événements cybernétiques. Grâce aux connaissances acquises par le truchement de ce système automatisé, le MDN et les FAC peuvent créer, appliquer et surveiller leur cyberespace complexe et dispersé. La confirmation de la conformité aux normes peut être maintenue et le procédé technique par lequel le changement du cyberespace est mis en œuvre peut être quantifié et vérifié. La connaissance des entités du cyberespace permettra également la mise en œuvre de mesures de sécurité accrues autour des services essentiels identifiés ou des zones de vulnérabilité cybernétique connue essentielles aux opérations.

Le projet CD-AD vise à améliorer la capacité du MDN et des FAC de détecter, d'analyser et de partager des activités suspectes dans le cyberespace et, lorsqu'elles ont été décelées, d'appuyer le processus décisionnel pour les CD en déterminant les mesures d'intervention disponibles et leurs conséquences. De plus, il automatisera l'exécution des mesures d'intervention lorsqu'elles ont été approuvées ou préapprouvées.

L'objectif des projets est de créer collectivement une capacité durable de gestion de la cybersécurité défensive à la fine pointe de la technologie, composée de personnel du MDN et des FAC et des services professionnels, habilités avec une gouvernance et une politique appropriées, et dotés des outils et des processus adéquats.

1.3 Premières lettres d'intérêt

Le 16 décembre 2016, les deux projets ont publié leurs premières lettres d'intérêt (LI)[5]. L'intention était d'informer et de préparer l'industrie pour les occasions d'approvisionnement potentielles dans le cadre de ces projets et d'obtenir des commentaires concernant la portée, les exigences, le calendrier, les risques et les coûts potentiels des projets.

Les réponses à ces LI ont aidé l'équipe du projet à parvenir aux conclusions générales suivantes :

a. Il existe un intérêt important dans l'ensemble de l'industrie de fournir des solutions pour les deux projets;
b. La technologie existe pour fournir des solutions pour les deux projets de manière opportune et rentable qui :

    1) Couvre l'ensemble du cycle de vie de la cyberattaque;

    2) Couvre l'architecture de réseau de l'infrastructure de technologie de l'information (ITI), des périphériques au noyau;

    3) Fournit une prise de décision fondée sur le renseignement;

    4) Traite des menaces et des vecteurs d'attaque pertinents pour la population;

    5) Cible les systèmes et les programmes pertinents pour la mission;

    6) Est en mesure de s'adapter à l'environnement, à l'architecture et aux contraintes des systèmes finaux;

    7) Utilise des normes ouvertes;

[5] Pour plus de renseignements sur les informations et les exigences initiales du projet, les répondants sont invités à se reporter à la première lettre d'intérêt publiée dans Achatsetventes.gc.ca (https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-QE-049-26099 et https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-QE-049-26100) le 16 décembre 2016.

8) Intègre à la fois les capteurs basés sur le réseau et le serveur, les flux de données, les registres et les systèmes de détection d'intrusion, de prévention des intrusions et d'antivirus;

9) intègre les signatures mixtes et la détection basée sur l'heuristique;

10) Fournit des chevauchements, des variables observables et des techniques complémentaires, le cas échéant;

11) Utilise un mélange de technologies de surveillance de l'ITI indépendantes avec des flux de données pertinents pour la sécurité;

12) Démontre que l'industrie est prête à remplir les rôles de fournisseur suivants :

   i. **Intégrateur de système principal**. Ces fournisseurs proposeraient des solutions de responsabilité totale du système (SRS) pour le projet, regroupant des sous-systèmes de composants nouveaux et existants dans un ensemble et assurant que ces sous-systèmes fonctionnent ensemble. L'intégrateur de système principal peut sous-traiter les responsabilités et la livraison de sous-systèmes et de produits spécifiques à d'autres fournisseurs, mais conservera la responsabilité globale du rendement des capacités du système. Ces fournisseurs auront besoin d'une compréhension détaillée et vaste des exigences liées à l'ITI du MDN et des FAC, de la sensibilisation à la cybersécurité et des cyberopérations défensives.

   ii. **Intégrateur de sous-système**. Ces fournisseurs proposeraient des solutions aux sous-systèmes spécifiques de la capacité totale. Les intégrateurs de sous-systèmes peuvent sous-traiter des responsabilités et la livraison de composants et de produits spécifiques à d'autres fournisseurs, mais conserveront la responsabilité globale du rendement de leur sous-système. Ces fournisseurs auront besoin d'une compréhension détaillée de l'ITI du MDN et des FAC dans les segments spécifiques du sous-système de cybersécurité et du sous-système des cyberopérations défensives et de leur relation avec la capacité totale.

   iii. **Fournisseur de produits**. Les fournisseurs de produits proposent des produits clé en main spécifiques qui peuvent être utilisés par un ou plusieurs sous-systèmes. Par conséquent, il ne serait normalement pas nécessaire de connaître les connaissances classifiées spécifiques de l'ITI du MDN et des FAC ni de la sensibilisation à la cybersécurité et des cyberopérations défensives;

13) L'industrie a noté le lien étroit entre les deux projets et, dans certains cas, la nécessité de les considérer de manière conjointe, potentiellement comme un projet unique;

14) Des informations plus détaillées sont requises par l'industrie pour soutenir un exercice raisonnable d'estimation des coûts;

15) Pour accomplir les tâches de collecte d'informations et apprécier les exigences de sécurité potentielles, il est essentiel de procéder à des échanges d'informations plus détaillés avec l'industrie afin de pouvoir analyser les solutions possibles, les risques et les estimations de coûts.

1.4 Besoins opérationnels préliminaires

Se reporter à l'annexe B pour une description des besoins opérationnels préliminaires. Notez que l'annexe B présente les besoins opérationnels actuels des projets de SC et des CD-AD dans une vue architecturale conceptuelle.

1.5 Situation actuelle

Se reporter à l'annexe C pour une description de la situation actuelle.

ANNEXE B:ÉNONCÉ DES BESOINS OPÉRATIONNELS PRÉLIMINAIRE

ANNEXE B : ÉNONCÉ DES BESOINS OPÉRATIONNELS PRÉLIMINAIRES

1 Introduction

1.1 Contexte

À titre d'énoncé des besoins opérationnels (EBO) préliminaires, ce document continuera à évoluer de concert avec la discussion avec l'industrie et les intervenants. L'intention est d'arriver à la fin de la phase de définition des projets, au début de 2019, avec un EBO approuvé pour une capacité militaire que l'industrie peut offrir. En vertu des politiques gouvernementales et ministérielles énumérées à l'appendice 1, l'effort de définition des besoins se poursuit jusqu'à ce que les besoins soient tous satisfaits. Par conséquent, le Canada peut décider de modifier, d'ajouter ou de supprimer des besoins. La demande de renseignements (DR) permet aux répondants de proposer des solutions. Les solutions ne doivent pas être contraintes par les éléments conceptuels décrits ici et doivent, le cas échéant, contribuer au raffinement des exigences, processus et flux de travail associés à chaque projet.

La définition des besoins est également un exercice de compromis avec des facteurs tels que l'abordabilité et la faisabilité. À cette fin, compte tenu de l'architecture et du concept d'opérations actuels décrits à l'annexe C, l'équipe de projet doit déterminer le coût total de possession indicatif (CPI) pour la capacité souhaitée, du déploiement à jusqu'à la fin du cycle de vie prévu de 10 ans.

1.2 Vision

Dans le but de sécuriser et de défendre le cyberespace des Forces armées canadiennes (FAC), la vision du projet de sensibilisation à la cybersécurité (SC) et des cyberopérations défensives - aide à la décision (CD-AD) est de fournir aux FAC une capacité durable à la fine pointe de la technologie pour mener des opérations de cybersécurité. Plus précisément, la capacité fonctionnera aux niveaux SECRET et TRÈS SECRET, fournissant une cyberdéfense pour les réseaux aux niveaux SECRET et DÉSIGNÉ en utilisant les données recueillies à partir de sources ayant une classification allant de NON CLASSIFIÉES à SECRET.

La capacité fournie sera composée du personnel du MDN et des FAC et des services professionnels, habilités avec une gouvernance et une politique appropriées, et dotés des outils et des processus adéquats. Appuyé par du soutien en service et de la formation réactifs, le résultat apporte les capacités de cybersécurité[1] et des cyberopérations défensives (CD) [2]des FAC à des normes de classe mondiale. L'intention est de fournir au commandant de la composante cybernétique des forces interarmées (CCCFI, tel que décrit à l'annexe C) la connaissance de la situation factuelle, les plans d'action disponibles et les effets opérationnels nécessaires afin de prendre des décisions en matière de cybersécurité et de CD fondées sur des données probantes.

Le plan est de fournir une capacité d'exploitation initiale, avec une sécurité informatique et un équivalent des CD au National Institute of Standards and Technology (NIST), niveau de maturité de sécurité informatique 5[3]. La capacité

---

[1] **Cybersécurité**. L'ensemble de technologies, de processus, de pratiques et de mesures d'atténuation et d'intervention conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés afin d'en assurer la confidentialité, l'intégrité et la disponibilité.

[2] **Cyberopération défensive**. Une opération défensive menée dans le cyberespace ou au moyen du cyberespace pour détecter, vaincre ou atténuer les actions offensives et exploitantes pour maintenir la liberté d'action.

[3] http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html

doit rester efficace, adaptée et en service tout au long de son cycle de vie de 10 ans; elle évoluera rapidement et sur demande pour prévenir les menaces et y réagir, et rester efficace malgré la constante évolution du domaine

1.3 Portée

Aux fins de la présente DR, les capacités requises sont actuellement concentrées sur la fourniture de fonctionnalités intégrées sur le domaine classifié et le domaine désigné déployé. Dans le présent document, toute référence au « domaine cybernétique du MDN et des FAC » ou au « cyberespace du MDN et des FAC » doit être prise dans ce contexte, étant entendu que la portée de la solution fournie doit pouvoir s'étendre afin d'inclure des domaines ou des données de réseau additionnels. L'annexe C fournit l'infrastructure représentative. Une évaluation additionnelle sera effectuée au cours de la phase d'analyse des options pour déterminer la portée du projet dans le domaine cybernétique plus vaste du MDN et des FAC.

La portée des exigences permet la vision ci-dessus en fournissant aux cyberopérateurs un environnement intégré unique qui permet la collaboration et la conduite de la cybersécurité et des CD dans de multiples domaines de classification variable. Cela inclut, mais sans toutefois s'y limiter, les personnes, les politiques, les processus et les outils nécessaires à la visualisation, à la gestion des tâches, à l'instruction individuelle et collective et à un référentiel de données accessible et exploitable menant à un domaine cybernétique défendable du MDN et des FAC.

1.4 Qualités opérationnelles

La capacité recherchée pour les deux projets doit posséder les qualités opérationnelles suivantes.

1.4.1 **Sensibilisation**

La possibilité de rassembler, de fusionner et d'afficher des informations de qualité et en temps opportun dans différents domaines de sécurité.

a. **Besoin**. La sensibilisation interdisciplinaire est primordiale pour la qualité des décisions prises en matière de cybersécurité et de cyberdéfense. Les données fusionnées provenant d'un nombre grandissant de sources sont nécessaires pour visualiser le domaine cybernétique du MDN et des FAC, en vue de faciliter le commandement de la force cybernétique.

b. **Résultats**. Une visualisation dégagée, persistante et maniable du cyberespace du MDN et des FAC - du niveau tactique au niveau stratégique - qui permet l'analyse et la prise de décision du commandement. Dans toutes les opérations, les informations du MDN et des FAC restent sécurisées.

1.4.2 **Réactivité**

La capacité d'intervenir lorsque cela s'avère nécessaire.

a. **Besoin**. Le MDN et les FAC doivent être en mesure d'exercer un contrôle autorisé sur la posture de sécurité du cyberespace soutenue et transformationnelle, dans toutes les instances opérationnelles et de développement, aux niveaux tactique, opérationnel et stratégique.

b. **Résultats**. Afin de déterminer, de caractériser et d'atténuer les menaces, les attaques et les vulnérabilités, le MDN et les FAC disposent d'une capacité dynamique, adaptable, réactionnelle et proactive qui analyse en permanence la posture de sécurité du cyberespace et prend en charge les interventions.

1.4.3 **Souplesse**

La capacité de soutenir plusieurs plans d'action et la liberté de manœuvre dans le cadre de ces plans.

a. **Besoin**. Une capacité opérationnelle qui est déployable, capable de fonctionner dans le contexte opérationnel des FAC; évolutive, modulaire et facilement élargie; et qui peut fonctionner efficacement dans un environnement interdomaines.

b. **Résultats**. Une capacité efficace, évolutive et durable dans l'ensemble des scénarios opérationnels des FAC et fonctionnelle dans l'environnement de cyberdéfense du MDN et des FAC.

1.4.4 **Résilience**

La capacité de se remettre des changements de réseau, des attaques, des malheurs, des dommages ou des perturbations déstabilisantes dans l'environnement cybernétique, opérationnel et naturel, et de s'y adapter.

a. **Besoin**. Une capacité qui peut facilement se remettre d'une situation opérationnelle, ou s'y adapter, tout en conservant une capacité de cybersécurité et de CD de qualité. La capacité tient compte des menaces actuelles et évolutives et de l'évolution des technologies dans le domaine cybernétique, assurant la confidentialité, l'intégrité et la disponibilité des informations opérationnelles et des informations sur la cybersécurité.

b. **Résultats**. Une capacité durable qui peut constamment soutenir les opérations de réseau, la cybersécurité et les CD dans un environnement hautement contesté.

1.4.5 **Innovation**

La capacité de faire de nouvelles choses ou de faire des choses anciennes d'une manière nouvelle.

a. **Besoin**. Une capacité efficace sur le plan opérationnel qui évolue continuellement et exploite les possibilités émergentes (telles que l'intelligence artificielle [IA], l'apprentissage par machine [AM] et les analyses avancées) grâce à de nouveaux processus, des outils évolutifs et une formation adaptative.

b. **Résultats**. Tout au long de son cycle de vie, une capacité de pointe qui évolue facilement avec l'environnement, la mission et la menace changeants, contribuant à la cybersécurité plus large du gouvernement du Canada (GC).

1.4.6 **Interopérabilité**

Toutes les entités de force se connectent sans difficulté ou s'échangent de l'information.

a. **Besoin**. Une capacité conjointe pour que plusieurs sources de données soient fusionnées et échangées au sein du MDN et des FAC, avec des alliés clés et parmi les partenaires, efficace sur le plan opérationnel dans l'infrastructure du cyberespace du MDN et des FAC existante et prévue. (GC, É.-U., Groupe des cinq, OTAN, Sécurité publique, Services partagés Canada [SPC], le Centre de la sécurité des télécommunications [CST] et le secteur privé)

b. **Résultats**. Une capacité technique et d'information qui permet des opérations harmonieuses au sein du MDN et des FAC et avec nos principaux alliés et partenaires.

2 Concept d’opération général

2.1 Introduction

En reconnaissant que de nombreux produits, concepts, outils, logiciels et matériel existent dans les secteurs des TI, de la cybersécurité et de la cyberdéfense dans leur ensemble, l'exigence opérationnelle est présentée dans une approche modulaire généralisée avec des fondements fonctionnels conceptuels ou des modules.

2.2 Vue opérationnelle

La Figure B - 1 fournit une vue opérationnelle de haut niveau du système souhaité où les cyberopérateurs sont le

personnel chargé de la cybersécurité et des cyberopérations défensives. Ces opérateurs sont en première ligne des opérations des FAC, en soutenant le CCCFI dans ses tâches. Se reporter à l'annexe C pour les lignes de commandement, de contrôle et de communication. En établissant la capacité, les autorisations organisationnelles, les politiques habilitantes et les processus opérationnels sont mis en place pour permettre à la capacité des opérations de cybersécurité défensives d'exécuter sa mission.

L'intention est de créer, d'équiper, d'organiser et de former une capacité du Centre d'opérations de cybersécurité qui défend les réseaux du MDN et de la FAC dans l'environnement sans interruption 24/7, tout en offrant une formation initiale, une formation continue, un développement professionnel et le mentorat des cyber opérateurs du MDN et de la FAC qui peuvent être déployés pour appuyer les opérations de cyber-sécurité et de défense du MDN et de la FAC au niveau national ou international.

Le concept actuel d'opérations permet à tous les cyberopérateurs et autres utilisateurs (gestionnaires, dirigeants, commandants et leur cadre) de réaliser leurs tâches dans un seul environnement intégré. Ces tâches comprennent, sans toutefois s'y limiter : le flux de travail, le suivi, l'analyse, l'alerte, la production de rapports, la connaissance de la situation, les interventions et l'instruction (individuelle et collective). Chaque cyberopérateur a accès à un outil de visualisation du tableau de bord commun, adapté à son rôle et à ses responsabilités particulières. D'autres membres du personnel, tels que les cadres ministériels, les commandants, les gestionnaires et d'autres éléments des opérations de réseau du MDN et des FAC (comme la Marine royale canadienne, l'Aviation royale canadienne, l'Armée canadienne, le CJOC, le COMFOSCAN et l'état-major interarmées stratégique) auraient également les droits et privilèges pour accéder à l'information et mener des actions en fonction de leurs rôles désignés et attribués au MDN et dans les FAC.

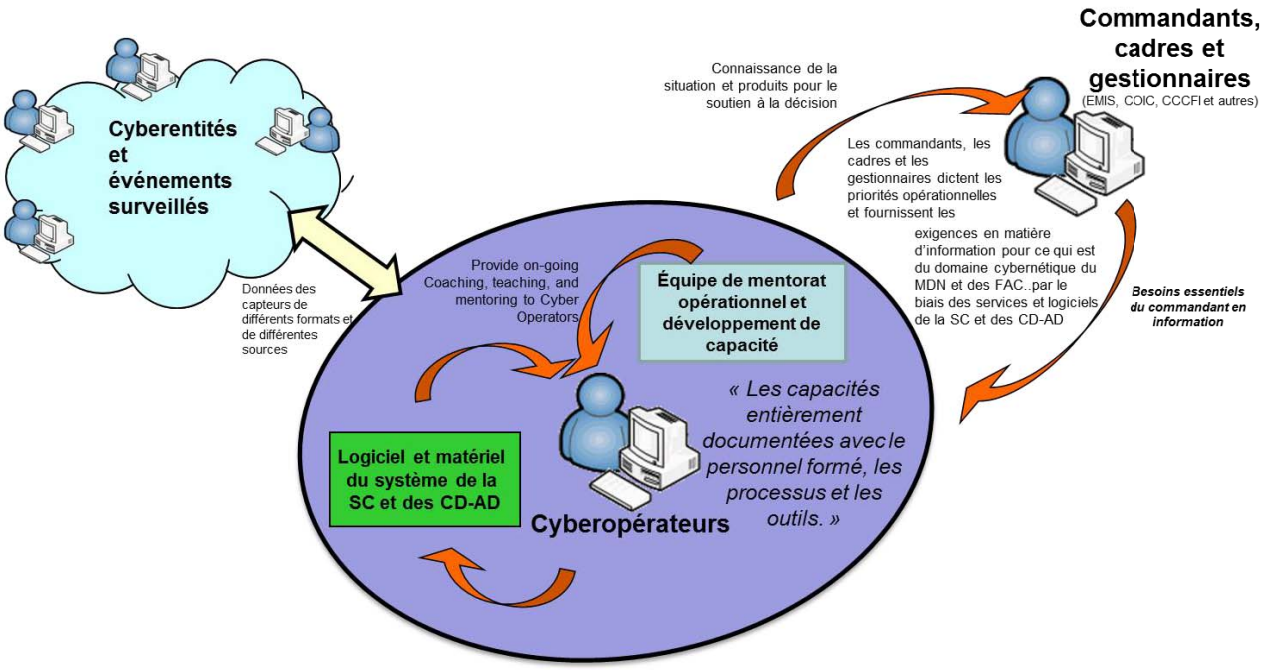

Figure B - 1 - Vue opérationnelle

2.3 Exigences fonctionnelles

2.3.1 **Principaux opérateurs et rôles**

Pour les CD, la solution proposée établira un environnement opérationnel 24 heures sur 24 et 7 jours sur 7, qui ne prévoit pas plus de dix (10) cyberopérateurs en service au même moment pour 10 000 utilisateurs dans un cyberespace du MDN et des FAC défini. Chaque équipe de quart comprend les analystes et spécialistes de sécurité de niveau 1, 2 et 3, [4]les analystes du renseignement cybernétique, un administrateur de système et un gestionnaire. On s'attend à ce que le ratio gestionnaire-personnel et le nombre d'employés varient en fonction de l'heure, du jour de la semaine et de la menace.

En s'appuyant sur des concepts traditionnels du centre d'opérations de cybersécurité et de l'industrie, et guidés par le mandat de la cyberdéfense des FAC, l'équipe mènera les CD grâce à la connaissance de la situation de la cybersécurité en temps opportun.

Dans le but de délimiter les activités essentielles, et en s'appuyant sur l'évolution de la doctrine interarmées, RDDC a énoncé les fonctions et tâches de la cyberdéfense en 2015. Cette analyse de la mission, des fonctions et des tâches a transformé les capacités de cyberdéfense requises en missions de cyberdéfense et leurs fonctions, puis permis d'énumérer les tâches nécessaires à l'exécution de chaque fonction. La Figure B - 2 présente les activités essentielles de cyberdéfense que les capacités de cybersécurité et des CD doivent affecter.

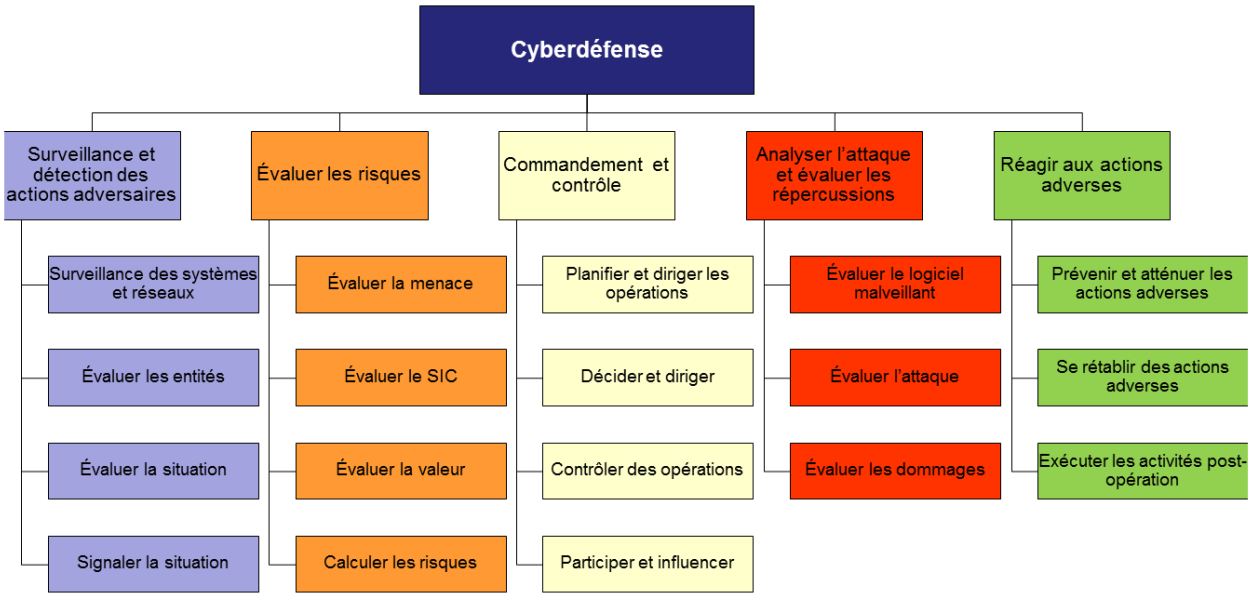

Figure B - 2 - Fonctions et tâches de cyberdéfense

[4] Tel que décrit dans Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, mai 2015, SANS institute : **Niveau 1** – Analyste d'alerte, **Niveau 2** – Intervenant, **Niveau 3** – Chasseur/Expert en la matière

2.3.2 **Mentorat opérationnel et développement de capacité (MODC)**

Les services professionnels, sous forme d'équipes de MODC, seront regroupés avec la capacité fournie pendant la mise en œuvre et tout au long de son cycle de vie. Le rôle des équipes de MODC est d'entraîner, de former et de guider les cyberopérateurs (de tous les grades) pour qu'ils réalisent leur mission grâce à la transformation opérationnelle continue, au développement des compétences, au développement et à la coordination de l'instruction collective, et au développement et au soutien des outils cybernétiques. L'équipe de MODC devra faire ce qui suit :

a. soutenir la transformation opérationnelle des capacités de cybersécurité et des CD des FAC afin qu'elles deviennent des capacités d'opérations de sécurité de niveau 5 du NIST;

b. soutenir les opérations de cybersécurité et les CD;

c. guider les cyberpérateurs à tous les niveaux pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences.

2.3.3 **Facilité d'estimation et d'évaluation de la capacité Cyber (FEECC)**

La tâche de la facilité d'estimation et d'évaluation de la capacité Cyber est de fournir au Centre des opérations de sécurité la possibilité d'exercer et de tester des solutions de cyber-défense et de sécurité dans un environnement simulé, représentatif du domaine cybernétique ciblé (c.-à-d. CSNI ou un autre domaine ou partie cybernétique de celle-ci) d'intérêt, pour prendre en charge les décisions relatives à d'autres enquêtes ou plans de mise en œuvre, le cas échéant.

La vision de la FEECC est de fournir des recherches sur la cybersécurité; des services de test et d'évaluation qui améliorent la position de la cybersécurité et portent sur l'évolution du paysage de la menace vers le domaine cybernétique du MDN et de la FAC. Pour atteindre la vision, le FEECC fournira un environnement évolutif et adaptable à l'appui:

a. L'identification et la validation des menaces et des risques liés à la cybersécurité en simulant le domaine cybernétique du MDN et de la FAC afin de déterminer l'impact sur la mission du MDN et du CAF.
a. L'intégration des capacités de cybersécurité, des outils et des technologies pour protéger les systèmes d'information, les données et l'infrastructure tout en satisfaisant les besoins stricts de sécurité, de sécurité et de disponibilité.
b. La transition vers une surveillance continue de l'environnement du système d'information pour détecter efficacement et efficacement les événements de cybersécurité.
c. L'amélioration des processus pour répondre et se remettre des événements et des attaques de la cybersécurité, y compris les attaques avancées et persistantes de groupes criminels et d'adversaires de l'État-nation.
d. Le processus d'évaluation et d'amélioration de la résilience de la capacité des systèmes d'information à exploiter et à exécuter la mission du MDN et de la FAC même s'il est affecté par un événement ou une attaque de cybersécurité.

La solution système FEECC sera:

a. Simulez exactement les performances de tous les domaines cybernétiques du MDN et de la FAC au niveau SECRET et ci-dessous, et fournit une configuration de la représentation de base de base managée de chaque facette de ces réseaux;

b. Fournir, dans les domaines cybernétiques du MDN et de la FAC sous évaluation, des évaluations de performance fiables et précises de:

1) Nouveau matériel et / ou logiciel,

2) modifications de la configuration du matériel et / ou du logiciel existants,

3) ajouts ou modifications de la nature et du nombre d'utilisateurs autorisés,

4) ajouts ou modifications aux points de présence et à leurs emplacements;

5) effets sur le débit de données et / ou la bande passante à n'importe quel point dans les réseaux,

6) la collecte des données du journal du système et des données SIEM, et

7) la distribution des données du journal du système et des données SIEM;

c. Intégrez-vous aux systèmes d'évaluation et d'évaluation du ITI du MDN et de la FAC existants ou prévus;

d. Améliorer la sensibilisation technique et la compréhension de la configuration et de l'exploitation des domaines cybernétiques existants du MDN et de la FAC; et

e. Améliorer l'identification des vulnérabilités dans les domaines cybernétiques du MDN et de la FAC existants.

2.4 Cyberentités

Une cyberentité est définie comme « toute chose distincte ou acteur distinct qui existe dans l'infrastructure cybernétique [cyberespace] ». [5] La connaissance de la situation cybernétique dépend donc de la « connaissance des cyberentités dans le cyberespace nécessaire pour prendre des décisions éclairées en matière de cybersécurité ».

Il existe deux types de cyberentités d'intérêt et il est essentiel que l'on découvre, obtienne, enregistre, surveille et maintienne autant d'attributs clés des cyberentités que possible :

a. **Cyberentités non humaines**. Ce sont des éléments du système participant (physiques ou virtuels) tels que les postes de travail, les routeurs, les commutateurs, les processus, les fichiers, les serveurs et la mémoire. Le tableau de l'appendice 2 de la présente annexe énumère les attributs clés qui doivent (le cas échéant) être collectés pour chaque cyberentité non humaine.

b. **Cyberentités humaines**. Ce sont des personnes réelles et leurs personnages opérant dans le cyberespace. Le tableau de l'appendice 3 de la présente annexe énumère les attributs clés qui doivent (le cas échéant) être collectés pour chaque cyberentité humaine.

2.5 Objectifs de rendement

Se basant sur les normes industrielles, le Tableau B - 1 démontre le rythme des activités du système général et de leurs objectifs de rendement pour ensuite fournir un critère d'efficacité préliminaire pour chacun.

Tableau B - 1 - Objectifs de rendement généraux

Rythme des activités	Objectif	Critère d'efficacité
En quelques secondes	• Repérer une cyberentité qui est active (connectée) dans le cyberespace du MDN et des FAC. (p. ex. : un ordinateur portable s'est connecté au réseau, un utilisateur s'est	• CE 1 : Mise à jour automatique de la cyberimage commune de la situation opérationnelle. • CE 2 : Le système possède des capacités de détection en temps quasi réel et peut détecter

[5] Source : Centre d'excellence de cyberdéfense coopérative de l'OTAN.

Rythme des activités	Objectif	Critère d'efficacité
	connecté, une clé USB a été branchée à un ordinateur, etc.) - SC • Éviter automatiquement une attaque contre le réseau ou le processeur central par l'utilisation d'un outil de protection comme le système de prévention des intrusions sur l'hôte (HIPS) - CD-AD • Créer une entrée de vérification et l'envoyer à la console de gestion des informations et des événements de sécurité (GIES) - CD-AD • Extraire automatiquement des fichiers d'une source telle que des pièces jointes d'un courriel ou un téléchargement du réseau, les exécuter dans une chambre de détonation et les analyser pour déceler des signes d'activités malveillantes - CD-AD • Déclencher une alerte dans le système de détection d'intrusion (SDI), puis envoyer l'alerte et les paquets associés à la console GIES - CD-AD	des événements cybernétiques anormaux dans l'ensemble du domaine cybernétique du MDN et des FAC. • CE 3 : La capacité suffisante de stockage les métadonnées de saisies du trafic du réseau, les registres, les alertes et les statistiques du domaine cybernétique du MDN et des FAC. • CE 4 : La capacité suffisante de surveiller tout le trafic du réseau, les métadonnées, les registres, les alertes et les statistiques du domaine cybernétique du MDN et des FAC. • CE 5 : La capacité d'appuyer le déroulement des analyses manuelles pour de multiples événements cybernétiques du domaine cybernétique accrédité du MDN et des FAC et des analyses en temps quasi réel des données pour signaler les cibles, les répercussions et les caractéristiques d'attaque. • CE 6 : Un processus d'analyse initiale automatisée en fonction des données antérieures, du renseignement et des menaces actuelles afin de prédire et de signaler les caractéristiques des événements cybernétiques, des attributions et des menaces futures éventuelles
En quelques minutes	• Déceler si la cyberentité détectée dans le cyberespace du MDN et des FAC est humaine ou non, et découvrir ses caractéristiques clés - SC • Cerner suffisamment de caractéristiques clés de la cyberentité détectée dans le cyberespace du MDN et des FAC pour déterminer son identité et sa position (physique et logique) précises - SC • Établir la caractéristique opérationnelle précise de la cyberentité détectée dans le cyberespace du MDN et des FAC pour la classer comme Ami, Ennemi ou Inconnu afin d'appuyer une décision d'engagement – CD-AD • Rechercher dans les registres mensuels pour tout système dans le cyberespace du MDN et des FAC et recueillir les résultats - CD-AD • Créer des tableaux croisés dynamiques pour aider les cyberopérateurs à identifier les entités avec un comportement malveillant	• CE 1 : Le contrôle et la mise à jour de l'endroit, l'activité et la configuration des appareils du réseau à fur et à mesure que des changements se font. • CE 2 : L'établissement de l'état de base du réseau et la connaissance de l'état du réseau. • CE 3 : La confirmation à distance des changements au réseau et au cyberespace pour surveiller leur implémentation. • CE 4 : Le jumelage des considérations de sécurité physiques et personnelles et des cybermenaces afin que des changements à la sécurité puissent être automatiquement approuvés, suivis et adaptés aux multiples vecteurs de menace. • CE 5 : La fonction du logiciel de protection et des systèmes sans qu'ils ne nuisent au domaine cyber.

Rythme des activités	Objectif	Critère d'efficacité
	similaire ou relié et avertir l'opérateur afin qu'il puisse amorcer des mesures d'intervention - CD-AD • Extraire les captures de paquets (PCAP) indexées d'une semaine de la mémoire en ligne avec des critères liés à l'entité comme des adresses IP, noms d'hôte, ports, comptes d'utilisateurs ou contenu - CD-AD • Reconnaître un événement inquiétant et le marquer comme anodin ou remplir un incident et l'envoyer au tiers 2[6] – CD-AD • Isoler un hôte infecté – CD-AD • Déterminer, puis contacter l'administrateur de système, l'officier de la sûreté ou l'officier des opérations au site contenant le système lié à l'incident potentiel - CD-AD	• CE 6 : La fonction des systèmes de sécurité autonomes ou lorsque connectés au réseau. • CE 7 : L'autorisation d'accès automatique des nœuds lors de la reconnexion au réseau pour permettre une connexion de confiance avec l'appareil. • CE 8 : La capacité de mettre en œuvre automatiquement une mise à jour ou une mise à niveau, lorsque jugée nécessaire par un participant cybernétique associé. • CE 9 : L'interopérabilité (communication et connaissance de la situation partagée) avec le GC et les systèmes alliés. • CE 10 : Un compte rendu et une présentation des renseignements nécessaires pour les décideurs, y compris : o Données cybernétiques affectées; o Résultats d'analyse; o Mesures prises d'une réponse automatique; o Événements connus semblables, réponses précédentes et leçons retenues; o Mesures d'intervention prédéfinies connues; o Mesures d'intervention manuelles disponibles. • CE 11 : Un système pour recevoir un accusé de réception d'un échange de renseignement. • CE 12 : L'utilisation d'un système selon les normes pour ses capacités de conversion au besoin pour échanger des renseignements.
En une heure	• Développer, télécharger, mettre à l'essai et déployer les signatures SDI à une flotte de capteurs - CD-AD • Identifier, analyser et développer un plan d'intervention contre une intrusion dans de multiples systèmes ou comptes - CD-AD	• CE 1 : La gestion des configurations de toutes les cyberentités est effectuée, y compris les points d'accès, et les logiciels sont utilisés pour créer la base de référence. • CE 2 : La mise en œuvre automatique, au besoin, des modifications des configurations. • CE 3 : L'appui à évaluation des conséquences opérationnelles durant l'événement cybernétique.

[6] Tel que décrit dans Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, mai 2015, SANS institute : **Niveau 1** – Analyste d'alerte, **Niveau 2** – Intervenant, **Niveau 3** – Chasseur/Expert en la matière

Rythme des activités	Objectif	Critère d'efficacité
	• Fournir l'analyse de la charge utile pour une nouvelle souche de virus au tiers 2 et tiers 3[7] - CD-AD • Identifier et rétablir les capteurs ou les flux de données en panne - CD-AD • Réunir les intervenants et les informer des détails de l'incident majeur en cours - CD-AD	• CE 4 : Le rapport des mesures effectuées et le délai d'exécution.
En une journée	• Purger mensuellement/trimestriellement toutes les signatures déployées à la flotte SDI ou tout le contenu déployé à la console GIES - CD-AD • Mettre à l'essai et recommander des correctifs majeurs à l'entreprise - SC • Analyser et documenter le contenu du système impliqué dans l'incident majeur tout en adhérant aux normes de la chaîne de possession légale - CD-AD o Déployer une équipe d'intervention en cas d'incident o Récupérer les données o Trier les données • Extraire à distance les artefacts criminalistiques à des fins d'analyse et de preuve - CD-AD o Fichiers o Processus o Mémoire o Registre o Image du disque dur virtuel o Image du disque dur au niveau des bits • Évaluer les actions et les intentions potentielles d'un adversaire qui opère par des réseaux circonscrits - CD-AD	• CE 1 : L'évaluation des vulnérabilités externes - Le système a la capacité d'analyser les nouvelles cybermenaces et celles en évolution pour créer une évaluation quantifiée de l'impact qu'elles auront sur le réseau. • CE 2 : L'impact et le risque d'apporter des modifications au domaine cybernétique peuvent être mesurés et quantifiés.
En une semaine	• Rapporter les résultats d'analyse et présenter des preuves juridiquement recevables - CD-AD • Développer, déployer et rendre opérationnel des outils sur mesure complexes de détection et d'analyse comme ceux utilisés dans les scripts pour Perl et GIES - CD-AD	• CE 1 : L'évaluation des vulnérabilités internes - Réduction du temps nécessaire pour effectuer une évaluation d'impact afin d'approuver les modifications au domaine cybernétique. • CE 2 : La réduction du temps pour effectuer la certification des entités tentant de se connecter au réseau en raison de l'automatisation du génie et des demandes de changement du système.

[7] Tel que décrit dans Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, mai 2015, SANS institute : **Niveau 1** – Analyste d'alerte, **Niveau 2** – Intervenant, **Niveau 3** – Chasseur/Expert en la matière

Rythme des activités	Objectif	Critère d'efficacité
	• Réviser, examiner et créer une base de référence pour une procédure normale d'exploitation (PNE) pour une opération de cybersécurité défensive interne - CD-AD • Exercer les nouvelles procédures durant les quarts de travail des cyberopérateurs - CD-AD • Informer les cyberopérateurs des nouvelles menaces et vulnérabilités - CD-AD • Créer de nouvelles techniques de défense fonctionnelles avec les nouvelles tactiques, techniques et procédures - CD-AD	
En un mois	• Créer de nouvelles techniques de défense fonctionnelles avec des nouveaux outils pour traiter les menaces nouvellement identifiées et priorisées - CD-AD • Améliorer la posture de sécurité globale (politiques, processus, outils) du cyberespace vulnérable du MDN et des FAC pour traiter les menaces nouvellement identifiées et priorisées - SC	

Le Tableau B - 2 indique les critères et objectifs du niveau de rendement du système requis.

Tableau B - 2 - Critères et objectifs du niveau de rendement du système

Critères	Objectif
Pertes	• Aucune perte de paquets aux points de présence surveillés. • Aucune perte de journal des événements. • Aucune perte de renseignement. • Intégrité des données vérifiables.
Détection	• Empêcher les adversaires de détecter (et d'éviter) la présence des capacités de surveillance.
Livraison	• Assurer la livraison entière des événements de sécurité des appareils finaux au centre d'opérations de cybersécurité défensive tout en les protégeant d'accès ou de modification non autorisés.
Surviabilité	• Appuyer la surviabilité de la cybersécurité et les capacités des CD, même lorsque certains secteurs du cyberespace sont compromis ou contestés.
Confidentialité	• Protéger des divulgations non autorisées des documents et des registres de nature délicate maintenus par les capacités des opérations de la cybersécurité défensive.

3 Besoins opérationnels

3.1 Besoins opérationnels

Le Tableau B - 3 indique les besoins opérationnels des FAC.

Tableau B - 3 - Description des besoins opérationnels

N°	Exigence	Projet	Description
1	L'utilisateur doit établir et maintenir un inventaire des cyberentités autoritaires et une base de données de configuration pour le domaine cybernétique du MDN et des FAC	SC	• Le système doit fournir une base de données de l'inventaire des cyberentités sécuritaires et autoritaires. • Le système doit fournir un schéma du réseau facile à visualiser de toutes les cyberentités. • Le schéma du réseau doit inclure la découverte de cyberentités autorisées (par l'entremise d'un changement, d'une configuration ou d'une gestion des versions) et non autorisées (malveillants ou autres). • Le système doit utiliser une nomenclature définie pour l'identification des cyberentités. • Le système d'identification d'entité doit inclure le(s) type(s) de l'entité, les réseaux, l'entité virtuelle ou physique, l'application ou le logiciel, la configuration, les appareils de bordure, la criticité de l'entité, la zone physique, les renseignements sur la solution interdomaine (SID) et la possession (voir les appendices 2 et 3).
2	L'utilisateur doit pouvoir identifier les cyberentités dans le domaine cybernétique du MDN et des FAC	SC	• Le système doit offrir un processus et des outils automatisés pour identifier toutes les entités et leur configuration (autorisée ou non autorisée). • Le système doit valider l'identité des entités autorisées. • Le système doit offrir un processus et des outils automatisés pour réagir en cas de découverte d'entités non autorisées (p. ex. : zone spéciale hôte, jardin fermé).
3	L'utilisateur doit pouvoir identifier les cyberentités dans le domaine cybernétique du MDN et des FAC	CD-AD	• Le système doit offrir la capacité de détection et d'intervention Endpoint (EDR) avec les sous-exigences suivantes : a. Le système doit offrir une capacité de cueillette des données détaillées concernant l'état actuel de chaque appareil d'extrémité (comme les processus en cours d'exécution, les réglages de registres, les fichiers actuellement ouverts, les connexions actives au réseau, le compte d'utilisateur en cours d'utilisation et les détails matériels comme l'utilisation de la mémoire et du CPU). b. Le système doit offrir une capacité de cueillette des données criminalistiques (historiques) des appareils d'extrémités (comme les processus exécutés, les fichiers ouverts et créés, les applications/commandes/scripts utilisés, les comptes d'utilisateur utilisés et les applications installées). c. Le système doit offrir une capacité de cueillette à distance des images de la mémoire ou des fichiers pour une enquête judiciaire.

N°	Exigence	Projet	Description
			d. Le système doit offrir une capacité de cueillette à distance des images du disque dur (serveur, poste de travail ou portable) pour une enquête judiciaire.
4	L'utilisateur doit surveiller les cyberentités dans le domaine cybernétique du MDN et des FAC	SC	• Le système doit offrir un processus et des outils automatisés pour surveiller toutes les entités (autorisée ou non autorisée) connectées au réseau. • Le système doit fournir l'état physique et logique en plus de l'emplacement de l'entité surveillée. • Le système doit surveiller les comptes administratifs et évaluer régulièrement cette entité pour assurer la conformité et la cyberdéfense.
5	L'utilisateur doit déterminer la vulnérabilité des cyberentités dans le domaine cybernétique du MDN et des FAC	SC	• Le système doit offrir un processus et des outils automatisés pour évaluer l'impact des vulnérabilités connues (p. ex. : les données sur les expositions et les vulnérabilités communes) des entités dans le cyberespace. • L'évaluation de l'impact des vulnérabilités du système doit inclure le type d'entité dans le cyberespace du MDN et la configuration du système complet ou de la fonction. • L'évaluation de l'impact des vulnérabilités du système doit inclure la chaîne de cyberdestruction au complet. • L'évaluation de l'impact des vulnérabilités du système doit déterminer la possibilité que le système soit compromis selon les vulnérabilités connues. • Le système doit fournir l'appui en accordant la priorité à des mesures correctives en identifiant les entités critiques. • Le système doit enregistrer les observations, déclencher les alertes, puis générer des comptes rendus d'évaluation des vulnérabilités.
6	L'utilisateur doit déterminer la conformité de la configuration des cyberentités dans le domaine cybernétique du MDN et des FAC	SC	• Le système doit offrir un processus et des outils automatisés pour évaluer la conformité selon la base de référence des configurations autorisées de toutes les entités. • Le système doit appuyer l'établissement des priorités des mesures correctives en identifiant les entités critiques. • Le système doit avoir la capacité de permettre au cyberopérateur d'incorporer, de traiter et de détecter automatiquement les indicateurs d'un secteur compromis. • Le système doit enregistrer les observations, déclencher les alertes, puis générer des comptes rendus de la conformité des configurations.
7	L'utilisateur doit pouvoir corréler des sources de données multiples et des processus d'évaluation d'appui par l'entremise de rapports et de	CD-AD	• Le système doit offrir un processus et des outils automatisés pour incorporer les sources de renseignements autoritaires des données suivants : a. données sur l'identité de l'utilisateur accrédité; b. données sur l'identité de l'administrateur accrédité; c. données sur le renseignement des menaces;

N°	Exigence	Projet	Description
	requêtes sur mesure préfabriqués		d. données sur l'inventaire des entités; e. données sur les vulnérabilités; f. données sur la gestion de la configuration; g. données sur la GIES; h. données sur la PCAP; i. données criminalistiques; j. ensembles de données et métadonnées nouvellement définis; k. données d'évaluation de la sécurité et d'autorisation. • Les sources des données du système autoritaire seront hébergées sur les réseaux de sensibilité faible, moyenne et élevée. • Les nouvelles sources de données, les formats de données et les protocoles de communication doivent adhérer aux normes actuelles de l'industrie ou être appuyés par des API.
8	L'utilisateur doit avoir un poste de travail à interface configurable	SC CD-AD	• Le système doit offrir une interface configurable conviviale offrant une connaissance de la situation appropriée au rôle, aux fonctions et aux tâches du cyberopérateur. • Le système doit offrir un processus et des outils automatisés pour demander une évaluation sur mesure. • Le système doit offrir une méthode personnalisable pour visionner les résultats des rapports et envoyer des rapports et des alertes. • Le système doit permettre des évaluations établies ou sur demande. • Le système doit offrir un indicateur de priorité pour les tâches d'atténuation actuelles. • Le système doit offrir une interface d'utilisateur configurable pour accomplir des tâches d'aide à la décision et accéder aux outils selon les rôles, voir les états et envoyer des rapports et des mises à jour.
9	L'utilisateur doit pouvoir déterminer le risque que présentent les modifications proposées pour cyberentités actuelles du MDN et des FAC	SC	• Le système doit offrir un processus et des outils automatisés pour analyser l'impact que pourraient avoir les modifications proposées au cyberespace du MDN et des FAC. • Le système doit offrir des moyens automatisés pour rapporter l'impact des modifications proposées au cyberespace du MDN et des FAC. • Les modifications au cyberespace doivent inclure un moyen d'intervention aux menaces et l'ajout, la mise à jour ou la suppression de logiciel, de matériel de configuration ou de conception. • L'évaluation des risques amenés par les modifications doit incorporer les mises à jour au RFC et à la gestion de la configuration.

N°	Exigence	Projet	Description
10	L'utilisateur doit pouvoir exécuter toutes les tâches dans des environnements DIL (déconnecté, intermittent ou à faible bande passante)	SC CD-AD	• Le système doit offrir un moyen de faire une évaluation rapidement déployable et locale pour appuyer les environnements DIL (p. ex : navires, aéronefs, déploiement en milieu inhospitalier). • Le système doit offrir un moyen de faire une évaluation centralisée afin d'obtenir et de fusionner tous les renseignements des environnements DIL lorsqu'il est possible de se connecter au réseau. • Le système doit être assez flexible pour travailler avec des contraintes au niveau de la bande passante imposées par les opérations. • Le système doit offrir une autre méthode de transfert de renseignements pour favoriser les environnements DIL sans compromettre les renseignements lorsque les conditions de connectivité s'améliorent.
11	Optionnel : L'utilisateur doit avoir la capacité de surveiller et de comprendre la plateforme de TI et la technologie opérationnelle[8] des flux de données de sécurité	SC	• Le système doit incorporer les flux de données de la plateforme de TI dans la mesure autorisée, comme l'état de connectivité, la posture de sécurité et la configuration. • Le système doit incorporer les flux de données de la technologie opérationnelle dans la mesure autorisée, comme l'état de connectivité, la posture de sécurité et la configuration. • Tous les flux de données doivent être conformes aux normes définies d'interopérabilité à sources ouvertes.
12	L'utilisateur doit pouvoir exécuter toutes les tâches par l'entremise de flux des travaux et un système d'assignation automatisé	SC CD-AD	• Le système doit avoir les capacités d'assignation automatisée et de flux des travaux pour intervenir en cas d'alertes ou de déclenchement. • Le système doit intégrer les flux des travaux et définir les processus/liens entre les différentes organisations fonctionnelles. • Le système doit automatiser des tâches d'analyses répétitives. • Le système doit être capable de suivre et de surveiller un progrès. • Le système doit pouvoir identifier des entités critiques pour appuyer l'établissement des priorités des tâches.
13	L'utilisateur doit pouvoir surveiller et appliquer une requête sur les politiques de contrôle de document	SC	• Le système doit automatiser et appliquer l'utilisation de l'étiquetage des données du MDN et des FAC sur des types de fichiers précis pour appuyer l'inventaire des fonds de données et appuyer les vérifications de conformité aux politiques de sécurité.

[8] La **plateforme de TI** est la technologie qui exécute et contrôle la plateforme elle-même (p. ex. : CVCA, CANBus, bus 1553, commandes moteurs, SCADA)

La **technologie opérationnelle** est une technologie spécialisée qui se trouve dans la plateforme de TI, mais qu'y n'en fait pas partie comme telle (p. ex. : suite de surveillance, systèmes d'armes, radar)

<table>
<tr><th>N°</th><th>Exigence</th><th>Projet</th><th>Description</th></tr>
<tr><td>14</td><td>L’utilisateur doit pouvoir effectuer la gestion des risques de manière efficace</td><td>SC
CD-AD</td><td>• Le système va pouvoir identifier, définir, intégrer et automatiser les processus requis pour appuyer la gestion des risques pour le domaine cybernétique du MDN et des FAC (posture de sécurité continuelle et mesures d'intervention).
• Les processus et les outils du système de gestion des risques doivent inclure la catégorisation des renseignements, la sélection de contrôle de sécurité, l’évaluation des mesures de sécurité, la vérification de conformité de la configuration et le calcul du risque.</td></tr>
<tr><td>15</td><td>L’utilisateur doit pouvoir effectuer la gestion des correctifs</td><td>SC</td><td>• Le système doit automatiser un processus efficace et efficient de gestion des correctifs.
• Le processus de gestion du système des correctifs doit identifier, acquérir, installer et vérifier les correctifs pour tous les produits et les systèmes (commerciaux ou gouvernementaux).
• Le système de gestion des correctifs doit inclure tous les systèmes d'exploitation, les applications, les interrupteurs, les routeurs et les appareils.</td></tr>
<tr><td>16</td><td>L’utilisateur doit comprendre les renseignements consolidés sur les menaces</td><td>CD-AD</td><td>• Le système doit incorporer le(s) flux de service cybernétique d’OSINT durable, ajustable et de bonne réputation.
• Le système doit avoir une capacité automatisée, efficace et fiable de fusion des renseignements sur les menaces qui permet l’analyse de sources et de conditions multiples.</td></tr>
<tr><td>17</td><td>Le système doit fonctionner dans de multiples domaines de sécurité</td><td>SC
CD-AD</td><td>• Le système doit fonctionner dans un environnement SID pour les utilisateurs du MDN et des FAC (p. ex : de multiples domaines de sécurité sur un seul poste de travail).
• Le système doit fonctionner dans un environnement SID côté serveur du MDN et des FAC.</td></tr>
<tr><td>18</td><td>L’utilisateur doit pouvoir recueillir et analyser des données de trafic brutes</td><td>CD-AD</td><td>• Le système doit fournir toutes les données recueillies (hors bande) et conservées du trafic du réseau brut du cyberespace des FAC (interne, entrant, sortant);
• Dans le but d'établir les coûts, d'obtenir les conditions entrantes et d'établir les conditions de conception, considérer les directives de conservation de données suivantes :
<table>
<tr><th>Données</th><th>Tiers 1 :</th><th>Tiers 2 +</th></tr>
<tr><td>Alertes SDI et alertes connexes GIES</td><td>2 semaines</td><td>Plus de 5 ans</td></tr>
<tr><td>Registres NetFlow / SuperFlow</td><td>1 mois</td><td>Plus de 5 ans</td></tr>
<tr><td>Session complète PCAP</td><td>48 heures</td><td>Plus de 2 ans</td></tr>
<tr><td>Registres de vérification</td><td>48 heures</td><td>Plus de 5 ans</td></tr>
</table>
• Le système doit appuyer les analyses rétrospectives et les fonctions de vérification.</td></tr>
</table>

N°	Exigence	Projet	Description
19	L'utilisateur doit pouvoir faire le suivi du trafic du réseau et des détections d'événements en temps réel	CD-AD	• Le système doit offrir le suivi continu et l'analyse du trafic du réseau en temps réel pour créer une détection des événements selon leur signature et leur comportement. • Le système doit corréler l'activité de l'utilisateur entre les domaines et les oppositions. • Le système doit offrir la capacité d'enregistrer les observations, de déclencher les alertes, puis de générer des comptes rendus.
20	L'utilisateur doit pouvoir faire le suivi d'entité et des détections d'événements en temps réel	CD-AD	• Le système doit offrir le suivi continu et l'analyse de l'activité des entités en temps réel pour créer une détection des événements. • Le système doit offrir la capacité d'enregistrer les observations, de déclencher les alertes, puis de générer des comptes rendus.
21	L'utilisateur doit pouvoir faire le suivi des activités de l'utilisateur et des détections d'événements en temps réel	CD-AD	• Le système doit offrir le suivi continu et l'analyse des activités contextualisées de l'utilisateur en temps réel pour créer une détection des événements. • Le système doit offrir la capacité d'enregistrer les observations, de déclencher les alertes, puis de générer des comptes rendus.
22	L'utilisateur doit pouvoir faire la collecte et l'analyse des données d'entreprise	CD-AD	• Le système doit offrir la collecte continue, la consolidation et la corrélation des renseignements sur la sécurité et des registres d'événement des ressources en réseau d'un répertoire d'une petite entreprise afin de mettre en contexte et de fournir des métadonnées et des analyses, des manuels d'appui, et des requêtes et des rapports automatisés (prévus et ponctuels). • Le système doit offrir des analyses sur mesure des données antérieures à court terme (p. ex. : requête rédigée, modélisation de cas) et avoir la capacité d'enregistrer les observations, de déclencher les alertes, puis de générer des comptes rendus.
23	L'utilisateur doit pouvoir effectuer une analyse rétrospective	CD-AD	• Le système doit fournir une analyse des données d'entreprise pour détecter des activités suspectes ou anormales. • Le système doit fournir une corrélation entre les événements antérieurs, les tendances et les comportements, et les événements en temps réel afin de reconstruire les activités selon le contexte et les métadonnées. • Le système doit fournir les caractéristiques et les données pour appuyer la chasse aux menaces persistantes avancées (MPA), aux menaces intérieures et aux indicateurs. • Le système doit fournir des outils de vérification, un manuel d'appui, et des requêtes et des rapports automatisés (prévus ou ponctuels). • Le système doit fournir des analyses sur mesure des données antérieures à court terme (p. ex. : requêtes rédigées, modélisation de cas).
24	L'utilisateur doit pouvoir répondre aux alertes et aux déclenchements	SC CD-AD	• Le système doit répondre à des mesures précises et à des déclenchements.

N°	Exigence	Projet	Description
			• Le système doit rapporter les progrès et les observations au processus (ou sous-système ou module) d'où la tâche est provenue.
25	L'utilisateur doit pouvoir établir une intervention automatique ou semi-automatique aux événements	CD-AD	• Le système doit permettre l'exécution automatique d'interventions techniques prédéterminées pour des événements documentés qui dépassent les seuils documentés. • Le système doit offrir une commande manuelle prioritaire. • Le système doit produire des registres et des comptes rendus.
26	L'utilisateur doit avoir un flux des travaux d'intervention en cas d'incident	CD-AD	• Le système doit déterminer, définir et automatiser les processus et les flux de travaux requis pour une intervention en cas d'incident. • Le système doit produire des registres, des comptes rendus, des tâches et une gestion des tâches.
27	L'utilisateur doit pouvoir faire des enquêtes judiciaires tout en adhérant aux normes de la chaîne de possession numérique	CD-AD	• Les technologies et processus du système doivent être suffisants pour répondre aux exigences d'enquête du GC pour la chaîne de possession numérique.
28	L'utilisateur doit pouvoir échanger de l'information et des renseignements sur les menaces avec des partenaires, alliés et autres ministères.	SC CD-AD	• Les formats de données et les protocoles de communication du système doivent adhérer aux normes actuelles de l'industrie ou être appuyés par des API, comme : o Le CIDF (*Common Intrusion Detection Framework*); o L'IODEF (*Incident Object Description and Exchange Format*); o Le SDEE (*Security Device Event Exchange*); o Le WELF (*WebTrends Enhanced Log File*); o Le CEI/CBE (*Common Event Infrastructure/Common Base Event*); o Les CVE (vulnérabilités et expositions communes); o Le CEF (*Common Event Format*); o Le CEE (*Common Event Expression*); o Le STIX (*Structured Threat Information eXpression*); o Le TAXII (*Trusted Automated eXchange of Indicator Information*); o Le CYBOX (*Cyber Observable Expression*).

3.2 Composants fonctionnels théoriques

La capacité intégrée des projets de la SC et des CD-AD permettra l'exécution d'opérations de cybersécurité du MDN et des FAC et donnera la possibilité au JCCC de défendre les réseaux du MDN et des FAC en plus de diriger des cyberopérations. À cette fin, la ressource doit pouvoir effectuer plusieurs fonctions essentielles. Bien que plusieurs outils pour la cybersécurité soient nécessaires pour satisfaire aux exigences de la SC et des CD-AD, en théorie, les éléments ou composants clés fonctionnels recherchés peuvent être regroupés comme suit :

a. la capacité de créer et de maintenir une image commune de la situation opérationnelle (ICSO) exacte et à jour avec des rapports conventionnels et adaptés grâce à des aides visuelles comme un tableau de bord opérationnel cybernétique (*COD - Cyber Operational Dashboard*) et des gadgets logiciels;

b. la capacité de créer et de maintenir un dépôt des cyberdonnées (CDR) autoritaire comprenant des données de renseignements cybernétiques de multiples sources;

c. la capacité d'utiliser un outil automatisé de découverte de cyberentités et d'événements (*CEED - Cyber Entity and Even Discovery*);

d. la capacité d'utiliser un outil automatisé de surveillance et d'intervention en cybersécurité (*CSMA - Cyber Security Monitoring and Actions*);

e. la capacité d'analyser la cyberdéfense et prendre en charge des décisions (*CDADS - Cyber Defence Analysis and implement Decision Support*);

f. la capacité d'utiliser un outil automatisé de gestion des tâches (TM);

g. la capacité d'utiliser un outil intégré du système d'entraînement opérationnel (OTS) pour les cyberopérateurs.

Le Tableau B - 4 démontre chacun des composants fonctionnels théoriques.

Tableau B - 4 - Description des composants fonctionnels théoriques

Nº	Composant		Description
1	Tableau de bord opérationnel cybernétique	SC CD-AD	Le COD est une interface visuelle où tous les utilisateurs humains peuvent accéder aux renseignements conservés dans le dépôt des cyberdonnées afin d'améliorer la connaissance de la situation de la cyberdéfense et d'aider le traitement des incidents. Le COD contient des outils d'analyse graphique et un accès aux composants des systèmes CEED, CSMA, CDR, CDADS et TM. Le COD offre plusieurs tableaux de bord, vues dynamiques et des fonctions de rapports afin d'appuyer toutes les utilisations nécessaires aux utilisateurs concernés. Le COD peut être mis en œuvre comme une interface unique ou un ensemble de différentes applications selon le choix de conception et les contraintes de mise en œuvre. Le COD offre aussi des flux de données standard qui peut être utilisé par l'image commune de la situation opérationnelle (ICSO) existante et les applications de commandement et contrôle (C2) afin de visualiser la situation de la cyberdéfense avec les autres niveaux de la situation militaire comme les unités terrestres, aériennes et maritimes. Le terme « tableau de bord » fait référence à un affichage d'information à écran unique utilisé pour faire le suivi de l'état des cyberentités et de leurs comportements. Il peut présenter différents types d'affichages selon les exigences configurables de l'utilisateur. Les affichages peuvent être textuels, une liste de table textuelle, des graphiques à barres, des graphiques de tendance, une carte géographique, etc. Le tableau de bord permet aux utilisateurs clés (comme les gestionnaires, les cadres, les analystes, etc.) de voir l'état des cyberentités à partir de leur bureau. Le COD offre aussi des flux de données pour les systèmes de commandement et contrôle (C2) actuels en utilisant des formats de données standards tels que KML (Keyhole Markup Language) et NVG (NATO Vector Graphics). Sa capacité innovatrice permet l'intégration des données sur la cyberdéfense dans l'image commune de la situation opérationnelle (ICSO) militaire afin de combiner les domaines cybernétique et physique pour obtenir une connaissance de la situation générale. Le COD est l'endroit de travail principal pour tous les cyberopérateurs et les utilisateurs du dépôt des cyberdonnées. C'est au travers du COD que chaque cyberopérateur effectue et gère ses tâches (p. ex. : flux de travail, suivi des événements, bon de travail, analyses, saisie de données dans le CDR, gestion du CDR, etc.).

Nº	Composant		Description
2	Gestion des tâches	SC CD-AD	Ce composant comprend le système de gestion de l'allocation de tâches, des bons de travail et du flux de travail. Par l'entremise du COD, les cyberopérateurs et les gestionnaires appropriés peuvent utiliser le sous-système de la gestion des tâches pour avoir accès aux services de tâches, de bons et de flux de travail pour contrôler, suivre et gérer les travaux et les priorités des cyberopérateurs. La gestion des tâches permet aux superviseurs de quarts, aux gestionnaires, aux commandants et aux autres cadres de définir les tâches, les priorités de surveillance et les priorités de travaux en plus de réviser l'état des tâches, de gérer les horaires, d'administrer le flux de travail, etc.
3	Entraînement opérationnel	SC CD-AD	Ce composant d'entraînement est utilisé pour s'assurer que les cyberopérateurs, les gestionnaires, les cadres et les autres opérateurs sont à jour et maîtrisent leurs tâches, rôles et responsabilités dans le système intégré, y compris : a. la capacité de créer une simulation de menace, de pénétration et d'attaque opérationnelle pour exercer l'équipe de cyberopérateurs et évaluer leur état de préparation opérationnelle ainsi que leur efficacité; b. un composant d'entraînement opérationnel individuel axé sur les opérateurs individuels (tâches, rôles, progrès dans leur rôle); c. une formation axée sur les compétences et la validation des cyberopérateurs, opérateurs et civils dans leur rôle attribué autant au niveau individuel que collectif; d. un composant d'instruction collective pour une capacité d'opération de sécurité pour la cyberdéfense. Ceci est une réplique d'un ensemble de systèmes d'exploitation avec des ensembles de données hors ligne pour permettre une gamme complète de fonctions et de scénarios réalistes à des fins de formation.
4	Surveillance et intervention en cybersécurité	SC	Ce composant surveille continuellement le dépôt des cyberdonnées (CDR) pour identifier la présence de cyberentités non conformes, d'événements, d'alertes, de vulnérabilités ou autres changements à l'état des cyberentités dans le cyberespace du MDN et des FAC. Le système donne l'alerte aux cyberopérateurs adéquats lors de la présence de cyberentités ou comportements non conformes. Le sous-système réagit aussi aux alertes associées à la non-conformité pour donner l'autorisation aux configurations de cybersécurité des cyberentités et pour recommander une intervention corrective automatique (p. ex. : gestion des correctifs, mise à jour du système, jardin fermé, réduction d'utilisateurs ou des privilèges des applications, etc.) ou avec l'intervention d'un cyberopérateur. Ce composant effectue les activités essentielles liées à la sécurité comme la gestion des biens, l'évaluation des vulnérabilités, le contrôle de documents, la gestion de la configuration et les fonctions du changement de configuration telles que l'évaluation de la sécurité et le processus d'autorisation. Cela inclut aussi la mise en œuvre des contrôles de la sécurité critique (CSC) du centre de sécurité Internet (CIS) de 1 à 5 grâce aux interactions avec le CDR. Les éléments essentiels minimaux pour le CSC sont : 1. L'inventaire des appareils autorisés et non autorisés; 2. L'inventaire des logiciels autorisés et non autorisés; 3. La configuration sécuritaire des appareils des utilisateurs finaux; 4. L'évaluation et les mesures correctives continuelles des vulnérabilités; 5. L'utilisation contrôlée des privilèges administratifs.

Nº	Composant		Description
5	Analyse de la cyberdéfense et prise en charge des décisions	CD-AD	Ce composant surveille et analyse continuellement les dépôts de cyberdonnées (CDR) pour identifier de possibles vulnérabilités ou des cyberattaques et des intrusions dans le domaine cybernétique du MDN et des FAC. Le système donne l'alerte aux cyberopérateurs adéquats lors de la détection de vulnérabilités, de menaces, de risques ou de comportements. Il s'accorde automatiquement sans cesse pour réduire les faux positifs et les faux négatifs. Le système réagit aussi à toutes les cyberalertes et recommande au cyberopérateur des mesures correctives appropriées et leur impact. Il sera aussi capable d'automatiser l'exécution de mesures d'intervention préapprouvées. Le système permet : a. L'évaluation des facteurs de risque dynamiques (ERD) pour permettre aux intervenants de définir (et maintenir avec le temps) l'importance de leurs objectifs de mission et la dépendance de ceux-ci au cyberespace du MDN et des FAC. La capacité de l'ERD va corréler dynamiquement tous les renseignements fournis par le CDR afin d'évaluer continuellement les risques. La signature de risque sera disponible pour tous les utilisateurs pertinents de l'interface COD. b. La gestion des facteurs de risque dynamiques (DRM) pour appuyer les décideurs avec la gestion des risques qui sont identifiés par l'ERD. À cette fin, la capacité du DRM peut recommander une intervention individuelle ou un plan d'action complet en plus d'évaluer leur efficacité, leurs coûts et les effets secondaires relatifs aux objectifs de la mission. c. Les renseignements cybernétiques et l'analyse d'OSINT. d. La chasse et les analyses avancées. e. L'analyse criminalistique. f. Le traitement des incidents. g. L'intervention aux incidents avec une analyse d'un plan d'action. h. Le contrôle de la sécurité du réseau et la production de rapports. i. La planification opérationnelle.
6	Dépôt des cyberdonnées (CDR)	SC CD-AD	Une banque de données qui agit comme l'entrepôt pour les cyberentités autorisées et les données d'événements pour le cyberespace du MDN et des FAC. Il conserve toutes les données liées à la collection de toutes les cyberentités présentes dans le cyberespace du MDN et des FAC en plus d'une description de la relation entre ces entités en vue d'analyses des liens, d'analyses de vulnérabilités, de détection des intrusions, d'analyses criminalistiques et d'autres tâches relatives à la cybersécurité. La base de données comprend tous les outils de production de rapport sur les normes de l'industrie, de requête et d'analyse graphique. Le CDR a la capacité de stocker et de consolider tous les renseignements de différentes sources de données existantes requis pour les activités liées à la cyberdéfense. Tous les renseignements sont normalisés dans un modèle de données global et unifié selon les normes, puis rendus disponibles à toutes les applications qui en ont besoin. Le but principal du CDR est de consolider les renseignements à partir des outils et des produits existants qui ne sont pas interopérables et de permettre une corrélation globale pour les différentes activités liées à la cyberdéfense. Le composant est aussi la base pour produire une capacité de CD interopérable modulaire, flexible et agile.

Nº	Composant		Description
			Ce CDR rassemble, stocke et maintient toutes les sources et les renseignements cybernétiques de sources ouvertes et de services gouvernementaux, alliés, militaires et contractuels tout en fournissant une vue d'ensemble complète, exacte et à jour des menaces autant de nature cybernétique que non liée au domaine cybernétique du MDN et des FAC. Les sources de renseignement engloberont des flux sans classification à TRÈS SECRET. Pour des raisons de sécurité, cette base de données sera maintenue séparée du CDR. La base de données comprend tous les outils de production de rapport sur les normes de l'industrie, de requête et d'analyse graphique.
7	Cyberentités et découverte d'événements	SC CD-AD	Ce composant découvre, recueille et stocke toutes les données sur toutes les cyberentités et tous les cyberévénements, puis les stocke dans le CDR. Pour l'entrée manuelle des données, le système utilise le COD. Le système découvre et recueille des données selon une routine prédéfinie, soit automatiquement selon les modifications apportées aux données sur les cyberentités pour répondre aux alertes des systèmes de surveillance actuels ou à la demande d'un cyberopérateur. Le sous-système utilise la collection et la rétention de données de trafic brutes, le suivi du trafic du réseau et la détection d'événements en temps réel, le suivi de l'hôte et la détection d'événements en temps quasi réel, et le suivi des activités et la détection d'événements en temps quasi réel. Le tout est appuyé par une capture de l'ensemble des paquets à des points clés désignés dans le cyberespace du MDN et des FAC, où et quand il est possible.

La Figure B - 3 démontre la vue architecturale des composants notionnels décrits dans les modules ci-dessus.

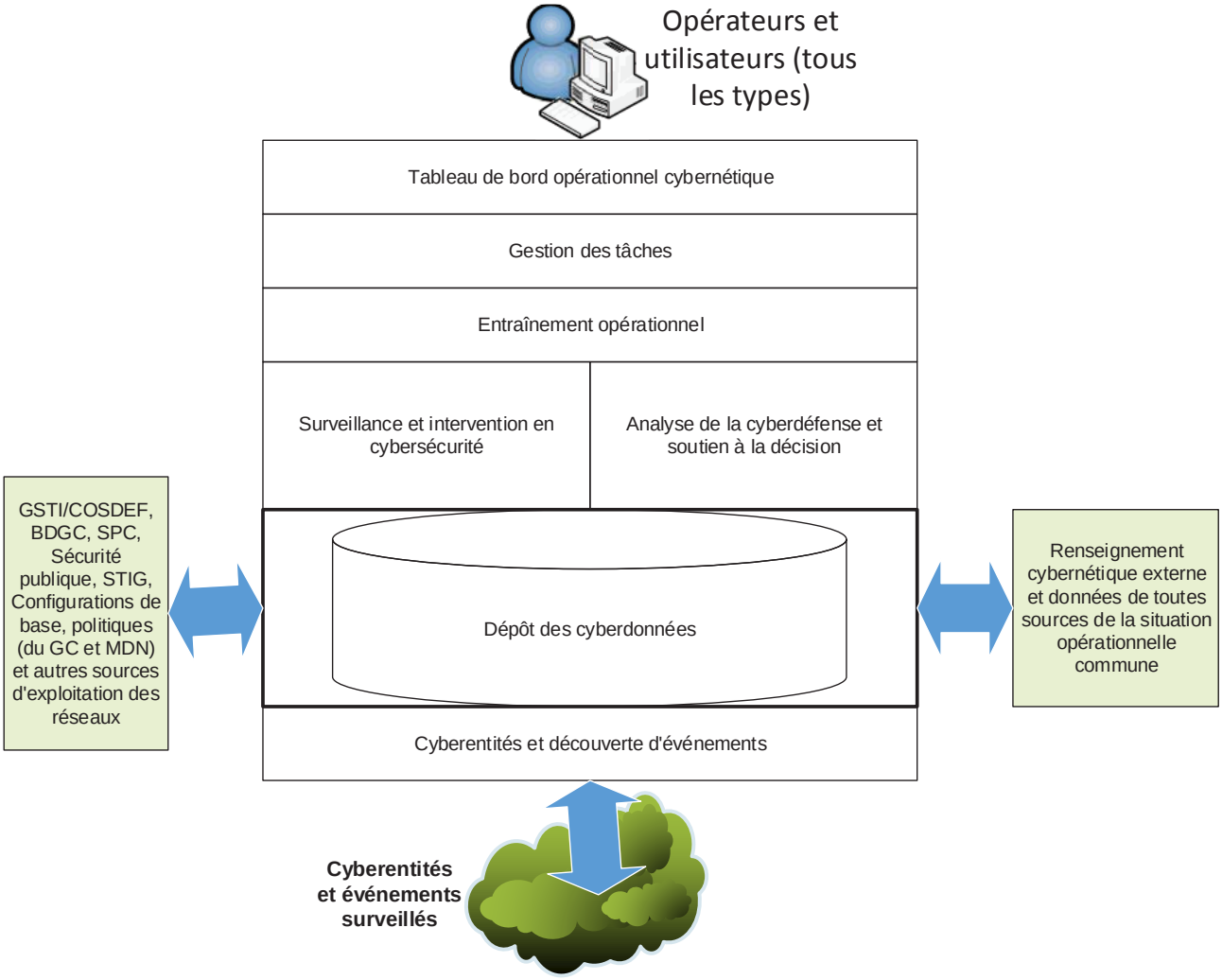

Figure B - 3 - Vue architecturale des composants notionnels

3.3 Contexte des exigences

L'environnement opérationnel des FAC est mondial et en constante évolution. Les CD sur le champ de bataille tactique exigent que les réseaux épisodiques, y compris leurs capacités de cybersécurité et de cyberdéfense, soient conçus de manière à ce qu'ils opèrent dans des conditions rudimentaires. Ceci comprend les déploiements lorsque les probabilités de déconnexion sont élevées dans des environnements épisodiques qui durent (instabilité lors du transport de l'infrastructure), dans des conditions à faible bande passante (navires) et dans la présence potentielle d'adversaires qui vont tenter de perturber les opérations en contestant l'utilisation du cyberespace des FAC.

Le déploiement nécessite un ensemble de compétences techniques spécifique pour opérer et maintenir. La chaîne de commandement doit s'assurer d'attribuer le bon nombre de personnel qualifié pour opérer ces capacités, au besoin, tout en maintenant une capacité centrale nationalement. Une configuration déployable commune maximise le rendement de l'instruction, du développent technique et des perspectives d'opérations de service et de génie.

Le déploiement dans un environnement de coalition ou de partenariat de mission nécessite que des instances épisodiques créées pour des événements liés à un déploiement de coalition ou de partenariat de mission soient le

volet canadien pour l'environnement de réseau de mission fédéré (RMF) établi. La cybersécurité et les capacités de CD déployées dans de tels environnements doivent pouvoir opérer au sein de la structure de gouvernance et de politique, comme convenu par la coalition.

Pour chaque besoin opérationnel décrit dans le Tableau B - 1, les composantes et/ou services doivent être conçus pour s'adapter à la nature changeante dynamique du domaine cybernétique. Il est acceptable qu'il ne soit pas possible de protéger l'entreprise de chaque vecteur de menace. Le but est de fournir un système qui peut résister aux attaques et continuer à livrer le commandement et contrôle essentiel, peu importe l'événement, tout en préservant la liberté opérationnelle d'action. À cette fin, les qualités décrites dans le paragraphe 1.4 doivent être reflétées dans la mise en œuvre de chaque besoin opérationnel.

3.4 Qualité et confidentialité des données

Dans chaque champ de données ou attribut recueilli, stocké ou déduit par analyse, un facteur de mérite de qualité et confidentialité des données est requis pour permettre une prise de décision judicieuse.

Lors de l'arrivée à l'évaluation de qualité et de confidentialité, considérer si les renseignements/données sont exacts, significatifs et opportuns. Le système doit fournir les mesures de confidentialité analytique appliquées pour :

a. La qualité et la confidentialité générales des renseignements selon les registres d'entités dans le CDR;
b. La connaissance généralisée de la situation, des alertes et l'état des bons aux plans d'intégrité des systèmes, l'état des incidents et les interventions;
c. La confidentialité des renseignements sur les menaces organisationnelles, stratégiques, opérationnelles, tactiques et techniques;
d. La confidentialité de l'évaluation des vulnérabilités.

Le facteur de mérite de qualité et de confidentialité devra prendre en compte :

a. La manière que les données ont été recueillies, rassemblées ou générées (la source);
b. Si les données ont été vérifiées indépendamment avec une ou plusieurs autres sources;
c. La probabilité que ces données peuvent changer au fil du temps;
d. Le moment auquel les données ont été recueillies ou vérifiées pour la dernière fois, soit sa déchéance.

Le facteur de mérite de qualité et de confidentialité sera qualifié par des termes clairs comme :

a. **Très peu probable**. 1 à 15 % de chance que les données soient vraies, complètes et exactes;
b. **Improbable.** 16 à 30 % de chance que les données soient vraies, complètes et exactes;
c. **Peu probable**. 31 à 45 % de chance que les données soient vraies, complètes et exactes;
d. **Possible.** 46 à 55 % de chance que les données soient vraies, complètes et exactes;
e. **Probable.** 56 à 70 % de chance que les données soient vraies, complètes et exactes;
f. **Très probable.** 71 à 85 % de chance que les données soient vraies, complètes et exactes;
g. **Presque certain**. 86 à 99 % de chance que les données soient vraies, complètes et exactes;
h. **Certain**. 100 % de chance que les données soient vraies, complètes et exactes.

3.5 Sécurité

Les solutions doivent être mises en œuvre de manière à soutenir les capacités qui fonctionnent aux niveaux SECRET et TRÈS SECRET, fournissant une cyberdéfense pour les réseaux aux niveaux SECRET et DÉSIGNÉ en utilisant les données recueillies à partir de sources NON CLASSIFIÉES vers SECRET.

3.6 Évaluation de la sécurité et autorisation

Les solutions doivent être mises en œuvre conformément aux lignes directrices de l'évaluation de la sécurité et d'autorisation (ESA) du MDN et des FAC (disponibles sur demande). Le processus d'ESA sera mené pour assurer la promulgation de directives appropriées par rapport à la mise en œuvre de matériel, de logiciels, de personnel et des procédures nécessaires pour satisfaire aux exigences des capacités de sécurité.

Les fournisseurs et sous-traitants peuvent nécessiter l'accès aux données et systèmes de nature délicate, nécessitant ainsi des attestations de sécurité de niveau approprié pour leur personnel et leurs installations.

Les fournisseurs et sous-traitants peuvent être tenus de se conformer à des ententes de non-divulgation ou d'autres restrictions liées à la sécurité.

Compte tenu de la menace associée au domaine cybernétique, un approvisionnement continu, fiable et garanti des biens et des services requis dans le cadre du projet doit être assuré en tout temps.

3.7 Surviabilité

Les solutions doivent se servir de fonctions qui minimisent la perturbation des opérations causée par des défectuosités d'un composant de toutes sortes.

3.8 Service et soutien

Le déploiement et le soutien des solutions doivent être intégrés dans les processus de configuration et de gestion du changement au sein du MDN et de SPC.

Le soutien doit être coordonné par l'intermédiaire de l'interconnectivité actuelle et future fournie par SPC.

Les solutions doivent donner les droits au MDN et aux FAC de créer, maintenir et modifier le logiciel d'interface sur mesure utilisé pour connecter les sources d'information dans la capacité.

Les solutions doivent pouvoir incorporer les mises à jour aux fonctions sans qu'il s'agisse de tâches d'ingénierie des logiciels majeures.

Les solutions doivent pouvoir être soutenues avec un minimum d'instruction supplémentaire au personnel de soutien.

Les solutions doivent pouvoir quadrupler le nombre de points d'extrémité sans mise à jour au système dorsal, à l'infrastructure, aux composantes, au matériel et aux logiciels actuels.

3.9 Disponibilité opérationnelle

La disponibilité de la capacité des composantes essentielles, mis à part les postes de travail (en présumant que l'utilisateur peut changer de poste de travail), est :

a. Obligatoire : 99,9 % du temps;
b. Souhaitable : 99,99 % du temps.

3.10 Fiabilité

Le système doit avoir une moyenne des temps de bon fonctionnement (MTBF) de 100 jours.

Le système doit être réparé et fonctionner en temps opportun conformément à l'énoncé de sensibilité et au

processus d’ESA.

3.11 Viabilité de l’environnement

Les solutions doivent satisfaire aux normes de gérance environnementale du MDN.

3.12 Santé et sécurité

Les solutions ne doivent pas causer d’autres préoccupations sur le plan de la santé et de la sécurité que celles qu’impose l’environnement d’exploitation, pour les opérateurs.

Les solutions doivent être conformes avec tous les codes de santé et sécurité du MDN et des FAC.

3.13 Exigences sur le plan de la livraison

Les solutions doivent comprendre des correctifs sécuritaires et un mécanisme de mise à jour accessibles partout dans le monde à partir d’endroits et de ressources approuvés.

Les solutions doivent soutenir et permettre l'accès à tous les utilisateurs (autorités opérationnelles, cyberopérateurs, personnel de soutien) qui opèrent et se trouvent dans une zone géographique ou un endroit de service situé dans la région de la capitale nationale (RCN).

Les solutions doivent soutenir et permettre l'accès à tous les utilisateurs (autorités opérationnelles, cyberopérateurs, personnel de soutien) qui opèrent et se trouvent :

a. à l’extérieur de la zone géographique ou de l'endroit de service situé dans la RCN, mais à l’intérieur du Canada;
b. à l’extérieur de la zone géographique ou de l'endroit de service situé dans la RCN, mais qui ont été déployés à l'étranger dans un endroit de service défavorisé avec des capacités de bande passante limitées.

3.14 Exigences relatives au personnel et à la formation

Les solutions doivent dispenser toute la formation nécessaire aux utilisateurs appropriés qui représentent l’autorité opérationnelle, aux cyberopérateurs et au personnel de soutien, conformément aux politiques et normes de formation des FAC et aux conclusions de l'évaluation des besoins de formation. Ceci englobe les installations, le matériel de formation et les formateurs qualifiés nécessaires pour atteindre la capacité opérationnelle initiale et un système d’instruction continue pour assurer une capacité opérationnelle totale.

Les solutions doivent dispenser une capacité de simulation de formation pour appuyer l’instruction opérationnelle collective dans un contexte opérationnel personnalisable. Les scénarios pour les simulations de formation doivent être créés, maintenus, modifiés et exécutés par les cyberopérateurs à partir des systèmes et des postes de travail actuels dans un environnement de formation ou d'exercice.

Les solutions doivent saisir les pratiques exemplaires et mettre en œuvre l’apprentissage fondé sur les connaissances des opérations et mesures précédentes.

4 Produits livrables préliminaires du contrat

Après avoir fourni les coûts indicatifs définis dans l’annexe D, les répondants doivent planifier la livraison des produits livrables du contrat suivants :

a. **Gestion de projet, ingénierie d'intégration et documentation du système :**

1) Plan de gestion de projet général;
2) Plan d'intégration (le rôle de l'intégrateur du sous-système ou du système principal);
3) Plan de mise à l'essai et de conformité;
4) Plan de transformation des activités;
5) Toute la documentation d'ingénierie des systèmes nécessaire.
6) Plans d'instruction et matériel de formation avec les outils en ligne dans le cyberespace du MDN et des FAC :
   i. Formation des membres du cadre initial d'instructeurs, axée à la fois sur l'instruction individuelle et collective des cyberopérateurs;
   ii. Formation continue, axée à la fois sur l'instruction individuelle et collective des cyberopérateurs;

b. **Composants fonctionnels théoriques**. Tous les matériaux et les logiciels nécessaires pour fournir les capacités prévues du fournisseur, comme ils ont été installés, configurés, mis à l'essai et acceptés, pour répondre à l'intention des exigences fonctionnelles définies dans l'annexe et conformément à la vue architecturale conceptuelle.

c. **Formation des membres du cadre initial d'instructeurs** pour chaque composante fonctionnelle selon les quantités inscrites dans l'annexe D.

d. **Services de transformation des activités.** Services professionnels nécessaires à la transformation des unités et du personnel d'opération pour fournir les capacités définies;

e. **Soutien en service et services professionnels d'ingénierie** pour une période de 10 ans après l'atteinte de la capacité opérationnelle finale, pour le personnel de soutien contractuel, les matériaux, les logiciels, les licences ou les abonnements et tous les services professionnels de soutien d'ingénierie pour la capacité en entier, avec des taux quotidiens par catégorie. Ces services doivent inclure un soutien planifié récurrent avec des services « sur appel » pour traiter des incidents urgents ou importants ou des interventions.

f. **Disposition d'une équipe de mentorat opérationnel et développement de capacité.** Comme décrit dans le paragraphe 2.3.2.

g. **Disposition d'une facilité d'estimation et d'évaluation de la capacité Cyber**. Comme décrit dans le paragraphe 2.3.3.

APPENDICE 1 DE L' ANNEXE B - POLITIQUES

1 Politiques habilitantes :

Il y a plusieurs politiques gouvernementales et ministérielles qui permettent une cybersécurité efficace et des cyberopérations défensives des FAC.

1.1 Politiques du gouvernement du Canada

a. Politique de défense du Canada « Protection, Sécurité, Engagement », 7 juin 2017, http://dgpaapp.forces.gc.ca/fr/politique-defense-canada/docs/rapport-politique-defense-canada.pdf

b. Politique sur la sécurité du gouvernement, Secrétariat du Conseil du Trésor du Canada, 1er avril 2012, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

c. Directive sur la gestion de la sécurité ministérielle, Secrétariat du Conseil du Trésor du Canada, 7 juillet 2009, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16579

d. Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI), Secrétariat du Conseil du Trésor du Canada, 31 mai 2004, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328

e. Norme opérationnelle sur la sécurité matérielle, Secrétariat du Conseil du Trésor du Canada, 18 février 2013, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329

f. Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC), Secrétariat du Conseil du Trésor du Canada, 11 décembre 2015, https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html

g. Cadre stratégique pour l'information et la technologie, Secrétariat du Conseil du Trésor du Canada, 9 juillet 2009, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12452

h. Plan fédéral d'intervention d'urgence, ministre de la Sécurité publique, janvier 2011, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-fr.aspx

i. Cadre de gestion des incidents cybernétiques pour le Canada, Secrétariat du Conseil du Trésor du Canada, 15 décembre 2015, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-fr.aspx

j. Plan stratégique de la technologie de l'information de 2016-2020, Secrétariat du Conseil du Trésor du Canada, 3 octobre 2016, https://www.canada.ca/fr/secretariat-conseil-tresor/services/technologie-information/strategie-technologie-information/plan-strategique-2016-2020.html

k. Cadre de politique sur la gestion des actifs et services acquis, Secrétariat du Conseil du Trésor du Canada, 23 mars 2012, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12022

l. Politique sur la gestion du matériel, Secrétariat du Conseil du Trésor du Canada, 26 juin 2006, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12062

1.2 Politiques ministérielles diverses

Dans le cadre de cette DR, les répondants doivent aussi présumer que les politiques suivantes existent :

a. Consentement de l'utilisateur à la surveillance : Donne aux cyberopérateurs et aux auditeurs la capacité sans équivoque de surveiller toutes les activités et de conserver l'information sur tous les systèmes et réseaux du MDN et des FAC;

b. Politique sur l'utilisation acceptable : Règles de comportement sur l'utilisation du système de TI, y compris les restrictions sur l'Internet et les sites de réseaux sociaux en plus de l'utilisation des logiciels autorisés sur les systèmes du MDN et des FAC;

c. Politiques sur la confidentialité et le traitement des données de nature délicate : Instructions pour gérer et protéger les types de renseignements qui traversent le réseau contrôlé, y compris des renseignements personnels, sur la santé, sur les finances et sur la sécurité nationale;

d. Ports et protocoles permis à l'interne : Énumération des ports et des protocoles permis dans le réseau du MDN et des FAC, autant au centre qu'aux limites;

e. Ports et protocoles permis à l'externe : Énumération des ports et des protocoles auxquels l'accès est permis avec des appareils à partir des limites extérieures, par exemple à travers une zone démilitarisée (DMZ), aux partenaires d'entreprise et à l'Internet.

f. Conventions d'appellation des hôtes : Description des conventions pour nommer et comprendre le type et le rôle de base des ressources de TI selon leurs enregistrements DNS;

g. Autre politique en matière de configuration et de conformité des TI : Tout, de la complexité des mots de passe au fonctionnement des systèmes, doit être aguerri et configuré;

h. Politiques sur les dispositifs personnels et portables (au besoin) : Règlements qui gouvernent la façon dont les employés peuvent accéder aux réseaux, applications et données du MDN et des FAC avec du matériel de TI ou des appareils mobiles personnels;

i. Les systèmes d'exploitation, les applications et les images de système approuvés : La liste générale approuvée des systèmes d'exploitation, des applications et des bases des systèmes pour les hôtes de chaque type : ordinateurs de bureau, ordinateurs portables, serveurs, routeurs, commutateurs et appareils;

j. Balayage tierce autorisé : Règles pour aviser les centres d'opérations lorsqu'une autre organisation désire effectuer un balayage, par exemple pour les vulnérabilités et la découverte de réseaux;

k. Politiques de vérification : Description de haut niveau des types de systèmes qui doivent capturer quels types d'événements, la durée de conservation des données, le responsable qui doit examiner ces données et le responsable de la collecte et de la conservation des données , en soulignant la valeur des données recueillies pour le rendement;

l. Rôles et responsabilités des autres organisations en ce qui concerne l'intervention en cas d'incident :

1) Intervenants internes du MDN et des FAC :

i. chef d'état-major de la défense;

ii. sous-ministre;

iii. dirigeant principal de l'information (DPI);

iv. coordonnateur ministériel de la sécurité des TI;

v. agent de sécurité du ministère;

vi. commandant de la Force cybernétique;

vii. commandant de la composante cybernétique des forces interarmées (CCCFI);

viii. Centre d'opérations du service de défense;

ix. Centre de gestion des systèmes nationaux (CGSN);

x. Centres de gestion des systèmes régionaux (CGSR);

xi. Service national des enquêtes des Forces canadiennes;

xii. Unité nationale de contre-ingérence des Forces canadiennes;

xiii. Centre d'opérations de réseau et centre d'opérations de sécurité ministériels de niveau 1 :

1. Marine royale canadienne;
2. Armée canadienne;
3. Aviation royale canadienne;
4. Commandement des opérations interarmées du Canada;
5. Commandement des Forces d'opérations spéciales du Canada;
6. NORAD.

2) Intervenants externes du MDN et des FAC :

i. Services partagés Canada - Équipe de réponse aux incidents cybernétiques du gouvernement du Canada (ERIC-GC);

ii. Centre de la sécurité des télécommunications (CST);

iii. Sécurité publique Canada;

iv. OTAN et autres partenaires alliés.

m. Accords sur les niveaux de service (ANS) écrits, le cas échéant :

1) Exigences de disponibilité et capacité du réseau;

2) Plan de circonstance si les services de réseau contractuels échouent;

3) Alertes et restauration des pannes de réseau (incident) et temps d'acheminement et de comptes rendus;

4) Alertes et procédures correctives d'incidents en matière de sécurité et temps d'acheminement et de comptes rendus;

5) Compréhension claire des responsabilités de chaque partie pour mettre en œuvre, opérer et maintenir les contrôles ou mécanismes de sécurité mis en œuvre lors de l'achat des services de réseau.

n. Politiques juridiques : Par rapport à la classification des renseignements, à la confidentialité, à la conservation des renseignements, à l'admissibilité des preuves et aux témoignages lors des enquêtes et des poursuites liées à des incidents.

APPENDICE 2 DE L’ ANNEXE B - ATTRIBUTS CLÉS DES CYBERENTITÉS NON HUMAINES

Nº	Description
1	Type d'hôte - physique ou virtuel
2	Nom de l'hôte (conformément à la convention de dénomination utilisée)
3	Numéro de fabricant / numéro de série / numéro d'inventaire du matériel (avec la marque d'inventaire en corrélation avec le titulaire du compte)
4	Processeur (fabricant, numéro de série, modèle, etc.)
5	Mémoire (fabricant, numéro de série, modèle, etc.)
6	Inventaire et identification de toutes les unités remplaçables en ligne (URL) à bord de l'appareil (ports CDROM / DVDRW / USB, matériel / clavier / souris / moniteurs / adaptateurs de réseau, processeurs, cartes mères, alimentations, conteneurs / cadres, etc.)
7	Type ou objectif principal de l'appareil (poste de travail, routeur de bureau virtuel, commutateur, pare-feu, passerelle, filtre Web, système de détection d'intrusion, système de prévention des intrusions, contrôleur de domaine, points d'accès sans fil, serveurs d'applications, serveur Mai, bases de données, applications intranet, etc.)
8	Modèle de périphérique, sous-modèle, version
9	Adresse MAC (ou adresses si plus d'une interface) pour tous les types d'interfaces externes
10	Adresse IP et sous-réseau (fixe ou attribuée par le DHCP)
11	Nom de l'hôte de l’URL
12	Méthode d'attribution de l'adresse IP : DHCP, réservée par le DHCP ou attribuée par l'hôte fixe
13	Heure de l'hôte
14	Serveur temporel du réseau hôte (si configuré à distance)
15	Hôte de passerelle
16	DNS principal, alternatif, deuxième alternatif hôte
17	Serveur DHCP hôte
18	Serveur WINS hôte
19	Serveur mandataire Web hôte (le cas échéant)
20	Tables de routage hôtes
21	Tableaux de transfert des ports hôtes
22	Tables de traduction d'adresses réseau hôtes (TAR)
23	Domaine hôte
24	Contrôleur de domaine principal attribué
25	Contrôleur de domaine secondaire attribué
26	Active Directory (AD), protocole allégé d'accès annuaire (LDAP), X.500 Statut d'enregistrement
27	IPv4 -ou-IPv6
28	Droits d'autorisation d'hôte (propriétaire, administrateurs, utilisateurs, invités, etc.) et comment ils sont assignés ou contrôlés (répertoire local ou actif)
29	Données SNMP utilisées et numéro de version
30	État du protocole ICMP
31	Logiciel antivirus basé sur hôte et version

Nº	Description
32	Logiciel de prévention des intrusions basé sur hôte et version
33	Logiciel de détection des intrusions basé sur hôte et version
34	État du service de pare-feu basé sur l'hôte
35	Autorité de certification de l'hôte
36	Ports hôtes (ouvert, fermé, écoute, mode furtif)
37	Système d'exploitation et version
38	Version d'image de base (le cas échéant)
39	Inventaire des logiciels installés - haut niveau
40	Inventaire des logiciels installés - niveau détaillé - toutes les DLL et les exécutables de soutien, les fichiers de configuration et les modules logiciels ou les composants connexes.
41	Configuration de départ Hashcode (pour faciliter la détection de changement de configuration de départ)
42	Services en cours d'exécution sur le périphérique et les ports utilisés
43	Certificats de services hôte
44	Nom d'utilisateurs enregistrés et actuellement authentifiés
45	Lieu - Nom de lieu physique (comme dans la BFC Petawawa, bâtiment P114, salle 101, bureau 5) et son équivalent géodésique (latitude, longitude, altitude), ou tout simplement, s'il s'agit d'un appareil mobile, sa latitude, sa longitude et son altitude.
46	Propriétaire - titulaire du compte matériel
47	Source d'alimentation (principale, batterie interne, batterie externe)
48	Source du système d'alimentation de secours
49	Propriétés physiques - température, humidité
50	Rapports de vulnérabilité existants, menaces connues, historique des rapports associés aux événements ou aux incidents
51	Réseau nommé, enclave, sous-réseau, etc. auxquels l'appareil est directement branché
52	Date de la dernière vérification ou inspection ou du dernier examen
53	Accès ou emplacement des registres internes de l'appareil (le cas échéant) (GIES, SNMP, SCOM, etc)

APPENDICE 3 DE L’ ANNEXE B - ATTRIBUTS CLÉS DES CYBERENTITÉS HUMAINES

Nº	Description
1	Nom de l'utilisateur principal et les réseaux ou domaines auxquels il est branché.
2	Nom d'utilisateurs alternatifs (un ou plus) et les réseaux ou domaines auxquels ils sont branchés.
3	Remplir les sections pour le nom, le rang et les renseignements relatifs à l'identification selon le dossier personnel ou d'une manière qui peut être corrélée plus tard.
4	Service, CIDP ou numéro d’attestation de sécurité industrielle
5	Division, formation, unité, sous-unité, etc.
6	Lieu principal ou lieu de travail
7	Autres lieux de travail temporaires
8	Domaine principal ou point de rapport
9	Autres domaines temporaires ou points de rapport
10	Adresses courriels pour chaque domaine ou réseau
11	Autorisations ou droits propriétaires pour les utilisateurs, les fichiers, les dossiers, les réseaux, les appareils
12	Active Directory (AD), protocole allégé d'accès annuaire (LDAP), X.500 Statut d'enregistrement
13	Rapports de vulnérabilités actuelles comme les fichiers, dossiers de documents et courriels associés à la personne, menaces connues, historique des rapports associés aux événements ou incidents, historique des points de terminaisons utilisés.
14	Date de la dernière vérification ou inspection ou du dernier examen
15	Accès ou emplacement des rapports de données de l'utilisateur

ANNEXE C:CONCEPT D'OPÉRATION ACTUEL ET CAPACITÉS EN SERVICE (CLASSIFIÉ);

L’annexe C est classifiée : Les fournisseurs qui souhaitent obtenir un exemplaire de l’annexe C doivent satisfaire aux exigences de sécurité décrites à l’annexe E – Exigences relatives à la sécurité.

Le document sera remis en version imprimée seulement, en personne, aux fournisseurs qui assistent à une rencontre individuelle ou à la réunion de suivi en groupe. Les directives concernant l’inscription à une rencontre individuelle et à la réunion de suivi en groupe sont fournies à l’annexe I.

Les fournisseurs qui ne satisfont pas aux exigences de sécurité sont invités à demander d’être parrainés pour obtenir l’attestation de sécurité exigée, conformément à l’annexe J – Demande de parrainage pour une attestation de sécurité.

Annexe C est marchandises contrôlées: Étant donné que Annexe C nécessite la production de marchandises contrôlées ou l'accès à des marchandises contrôlées qui sont visées par la *Loi sur la production de défense,* L.R., 1985, ch. D-1, l'entrepreneur et tout sous-traitant sont avisés que, au Canada, seules les personnes inscrites, exemptées ou exclues en vertu du Programme des marchandises contrôlées (PMC) sont légalement autorisées à examiner, à posséder ou à transférer des marchandises contrôlées. L'entrepreneur trouvera des précisions sur la façon de s'inscrire au PMC à l'adresse : http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-fra.html

ANNEXE D:MODÈLE D'OFFRES ET D'ÉVALUATION DES PRIX DES PRODUITS;

ANNEXE D : MODÈLE D'OFFRES ET D'ÉVALUATION DES PRIX DES PRODUITS

Nº	Élément livrable	Produit livrable	Coût de base par unité (par utilisateur, appareil, ep, etc.)	Prix par unité						Remarques
				Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	
1	**Tableau de bord opérationnel cybernétique**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
2		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberopérateur ou cadre ou gestionnaire du MDN et des FAC	50		51 à 100		101 à 500		
3		Services de transformation des activités	Lot	1						
4		Système de soutien en service et services d'ingénierie professionnels	Lot	1		0		0		
5		Formation des membres du cadre initial d'instructeurs	par cyberopérateur ou cadre ou gestionnaire du MDN et des FAC	50		51 à 100		101 à 500		
6	**Gestion des tâches**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
7		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		
8		Services de transformation des activités	Lot	1						
9		Système de soutien en service et services d'ingénierie professionnels	Lot	1		0		0		
10		Formation des membres du cadre initial d'instructeurs	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		
11	**Entraînement opérationnel**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						

Nº	Élément livrable	Produit livrable	Coût de base par unité (par utilisateur, appareil, ep, etc.)	Prix par unité						Remarques
				Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	
12		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberopérateur ou cadre ou gestionnaire du MDN et des FAC	50		51 à 100		101 à 500		
13		Services de transformation des activités	Lot	1						
14		Système de soutien en service et services d'ingénierie professionnels	Lot	1		0		0		
15		Formation des membres du cadre initial d'instructeurs	par cyberopérateur ou cadre ou gestionnaire du MDN et des FAC	50		51 à 100		101 à 500		
16	**Surveillance et mesures de cybersécurité**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
17		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		
18		Services de transformation des activités	Lot	1						
19		Système de soutien en service et services d'ingénierie professionnels	Lot	1		0		0		
20		Formation des membres du cadre initial d'instructeurs	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		
21	**Analyse de la cyberdéfense et prise en charge des décisions**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
22		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		
23		Services de transformation des activités	Lot	1						

Nº	Élément livrable	Produit livrable	Coût de base par unité (par utilisateur, appareil, ep, etc.)	Prix par unité						Remarques
				Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	
24		Système de soutien en service et services d'ingénierie professionnels	Lot	1						
25		Formation des membres du cadre initial d'instructeurs	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		
26	**Dépôt des cyberdonnées**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
27		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberentité dans le domaine cybernétique du MDN et des FAC	1 à 10 000		10 001 à 25 000		25 001 à 150 000		
28		Services de transformation des activités	Lot	1						
29		Système de soutien en service et services d'ingénierie professionnels	Lot	1						
30		Formation des membres du cadre initial d'instructeurs	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		
31	**Cyberentités et découverte d'événements**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
32		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberentité dans le domaine cybernétique du MDN et des FAC	1 à 10 000		10 001 à 25 000		25 001 à 150 000		
33		Services de transformation des activités	Lot	1						
34		Système de soutien en service et services d'ingénierie professionnels	Lot	1						
35		Formation des membres du cadre initial d'instructeurs	par cyberopérateur du MDN et des FAC	50		51 à 100		101 à 500		

Nº	Élément livrable	Produit livrable	Coût de base par unité (par utilisateur, appareil, ep, etc.)	Prix par unité						Remarques
				Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	
36	**Facilité d'estimation et d'évaluation de la capacité Cyber**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
37		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberentité dans le domaine cybernétique du MDN et des FAC	1 à 10 000		10 001 à 25 000		25 001 à 150 000		
38		Services de transformation des activités	Lot	1						
39		Système de soutien en service et services d'ingénierie professionnels	Lot	1						
40		Formation des membres du cadre initial d'instructeurs	par cyberopérateur ou cadre ou gestionnaire du MDN et des FAC	50		51 à 100		101 à 500		
41	**Système intégré total**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						
42		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par cyberentité dans le domaine cybernétique du MDN et des FAC	1 à 10 000		10 001 à 25 000		25 001 à 150 000		
43		Services de transformation des activités	Lot	1						
44		Système de soutien en service et services d'ingénierie professionnels	Lot	1						
45		Formation des membres du cadre initial d'instructeurs	par cyberopérateur ou cadre ou gestionnaire du MDN et des FAC	50		51 à 100		101 à 500		
46	**Base de solution définie par le fournisseur**	Gestion de projet, ingénierie d'intégration et documentation sur la conception du système	Lot	1						

Nº	Élément livrable	Produit livrable	Coût de base par unité (par utilisateur, appareil, ep, etc.)	Prix par unité						Remarques
				Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	Nombre d'unités	Prix par unité	
47		Tout le matériel, les logiciels, l'installation, la configuration du système et les essais d'acceptation	par base de quantité définie par le fournisseur							
48		Services de transformation des activités	Lot	1						
49		Système de soutien en service et services d'ingénierie professionnels	Lot	1						
50		Formation des membres du cadre initial d'instructeurs	par base de quantité définie par le fournisseur							
51	**Équipe de mentorat opérationnel et développement de capacité**		Lot	1		1		1		

Remarque : Comme indiqué dans la section 7.4, section 4 - Commentaires et conseils généraux, paragraphe 6 du document principal, les répondants peuvent proposer des solutions applicables à SC, CD-AD ou les deux et indiquer si les solutions proposées rencontrent les besoins en tout ou en partie pour le projet sélectionné. Les répondants peuvent proposer des solutions qui ne sont pas nécessairement conformes aux composantes fonctionnelles théoriques décrits à l'annexe B, figure B-3 dans la vue architecturale notionnelle tant que la solution globale répond aux exigences. Les répondants sont invités à indiquer clairement comment chaque livrable est livré. Par exemple, si la livraison d'une capacité nécessite des unités matérielles et logicielles discrètes, du personnel de soutien ou du personnel du centre d'opérations, les répondants doivent clairement l'indiquer dans la base de coûts unitaires, le prix ou l'unité et le nombre d'unités requis. À tout le moins, la réponse doit indiquer que le coût de la solution se calcule facilement à l'aide du modèle simple suivant : Coût = prix / unité x nombre d'unités.

APPENDICE 1 DE L' ANNEXE D - ATTRIBUTS CLÉS DES CYBERENTITÉS NON HUMAINES

Nº	Description	Capacité			Remarques ou commentaires
		Conformité? (Conforme à la construction Partiellement conforme à la construction, Possible mais nécessite des efforts d'ingénierie, Non possible dans l'avenir prévisible, inconnu)	**Expliquer comment les données sont déterminées** (Entrée manuelle dans la BDGC, Analyse quotidienne des services des appareils connus, Analyse active des données existantes provenant de sources multiples, autres)	**Qualité et niveau de confiance dans l'élément de données** (À distance, très improbable, peu probable, chance égale, probable, très probable, presque certain, certain)	
1	Type d'hôte - physique ou virtuel				
2	Nom de l'hôte (conformément à la convention de dénomination utilisée)				
3	Numéro de fabricant / numéro de série / numéro d'inventaire du matériel (avec la marque d'inventaire en corrélation avec le titulaire du compte)				
4	Processeur (fabricant, numéro de série, modèle, etc.)				
5	Mémoire (fabricant, numéro de série, modèle, etc.)				
6	Inventaire et identification de toutes les unités remplaçables en ligne (URL) à bord de l'appareil (ports CDROM / DVDRW / USB, matériel / clavier / souris / moniteurs / adaptateurs de réseau, processeurs, cartes mères, alimentations, conteneurs / cadres, etc.)				
7	Type ou objectif principal de l'appareil (poste de travail, routeur de bureau virtuel, commutateur, pare-feu, passerelle, filtre Web, système de détection d'intrusion, système de prévention des intrusions, contrôleur de domaine, points d'accès sans fil, serveurs d'applications, serveur Mai, bases de données, applications intranet, etc.)				
8	Modèle de périphérique, sous-modèle, version				
9	Adresse MAC (ou adresses si plus d'une interface) pour tous les types d'interfaces externes				
10	Adresse IP et sous-réseau (fixe ou attribuée par le DHCP)				
11	Nom de l'URL de l'hôte				
12	Méthode d'attribution de l'adresse IP : DHCP, réservée par le DHCP ou attribuée par l'hôte fixe				
13	Heure de l'hôte				
14	Serveur temporel du réseau hôte (si configuré à distance)				

Nº	Description	Capacité			Remarques ou commentaires
		Conformité? (Conforme à la construction Partiellement conforme à la construction, Possible mais nécessite des efforts d'ingénierie, Non possible dans l'avenir prévisible, inconnu)	**Expliquer comment les données sont déterminées** (Entrée manuelle dans la BDGC, Analyse quotidienne des services des appareils connus, Analyse active des données existantes provenant de sources multiples, autres)	**Qualité et niveau de confiance dans l'élément de données** (À distance, très improbable, peu probable, chance égale, probable, très probable, presque certain, certain)	
15	Hôte de passerelle				
16	DNS principal, alternatif, deuxième alternatif hôte				
17	Serveur DHCP hôte				
18	Serveur WINS hôte				
19	Serveur mandataire Web hôte (le cas échéant)				
20	Tables de routage hôtes				
21	Tableaux de transfert des ports hôtes				
22	Tables de traduction d'adresses réseau hôtes (TAR)				
23	Domaine hôte				
24	Contrôleur de domaine principal attribué				
25	Contrôleur de domaine secondaire attribué				
26	Active Directory (AD), protocole allégé d'accès annuaire (LDAP), X.500 Statut d'enregistrement				
27	IPv4 -ou-IPv6				
28	Droits d'autorisation d'hôte (propriétaire, administrateurs, utilisateurs, invités, etc.) et comment ils sont assignés ou contrôlés (répertoire local ou actif)				
29	Données SNMP utilisées et numéro de version				
30	État du protocole ICMP				
31	Logiciel antivirus basé sur hôte et version				
32	Logiciel de prévention des intrusions basé sur hôte et version				
33	Logiciel de détection des intrusions basé sur hôte et version				
34	État du service de pare-feu basé sur l'hôte				
35	Autorité de certification de l'hôte				
36	Ports hôtes (ouvert, fermé, écoute, mode furtif)				
37	Système d'exploitation et version				

Nº	Description	Capacité			Remarques ou commentaires
		Conformité? (Conforme à la construction Partiellement conforme à la construction, Possible mais nécessite des efforts d'ingénierie, Non possible dans l'avenir prévisible, inconnu)	**Expliquer comment les données sont déterminées** (Entrée manuelle dans la BDGC, Analyse quotidienne des services des appareils connus, Analyse active des données existantes provenant de sources multiples, autres)	**Qualité et niveau de confiance dans l'élément de données** (À distance, très improbable, peu probable, chance égale, probable, très probable, presque certain, certain)	
38	Version d'image de base (le cas échéant)				
39	Inventaire des logiciels installés - haut niveau				
40	Inventaire des logiciels installés - niveau détaillé - toutes les DLL et les exécutables de soutien, les fichiers de configuration et les modules logiciels ou les composants connexes.				
41	Configuration de départ Hashcode (pour faciliter la détection de changement de configuration de départ)				
42	Services en cours d'exécution sur le périphérique et les ports utilisés				
43	Certificats de services hôte				
44	Nom d'utilisateurs enregistrés et actuellement authentifiés				
45	Lieu - Nom de lieu physique (comme dans la BFC Petawawa, bâtiment P114, salle 101, bureau 5) et son équivalent géodésique (latitude, longitude, altitude), ou tout simplement, s'il s'agit d'un appareil mobile, sa latitude, sa longitude et son altitude.				
46	Propriétaire - titulaire du compte matériel				
47	Source d'alimentation (principale, batterie interne, batterie externe)				
48	Source du système d'alimentation de secours				
49	Propriétés physiques - température, humidité				
50	Rapports de vulnérabilité existants, historique des rapports associés aux événements ou aux incidents				
51	Réseau nommé, enclave, sous-réseau, etc. auquel l'appareil est directement branché				
52	Date de la dernière vérification ou inspection ou du dernier examen				
53	Accès ou emplacement des registres internes de l'appareil (le cas échéant) (GIES, SNMP, SCOM, etc)				

APPENDICE 2 DE L’ ANNEXE D - ATTRIBUTS CLÉS DES CYBERENTITÉS HUMAINES

Nº	Description	Capacité			Remarques ou commentaires
		Conformité? (Conforme à la construction Partiellement conforme à la construction, Possible mais nécessite des efforts d'ingénierie, Non possible dans l'avenir prévisible, inconnu)	**Expliquer comment les données sont déterminées** (**Entrée** manuelle dans la BDGC, Analyse quotidienne des services des appareilsconnus, Analyse active des données existantes provenant de sources multiples, autres)	**Qualité et niveau de confiance dans l'élément de données** (À distance, très improbable, peu probable chance égale, probable, très probable, presque certain, certain)	
1	Nom de l'utilisateur principal et les réseaux ou domaines auxquels il est branché.				
2	Nom d'utilisateurs alternatifs (un ou plus) et les réseaux ou domaines auxquels ils sont branchés.				
3	Remplir les sections pour le nom, le rang et les renseignements relatifs à l'identification selon le dossier personnel ou d'une manière qui peut être corrélée plus tard.				
4	Numéro matricule				
5	Division, formation, unité, sous-unité, etc.				
6	Lieu principal ou lieu de travail				
7	Autres lieux de travail temporaires				
8	Domaine principal ou point de rapport				
9	Autres domaines temporaires ou points de rapport				
10	Adresses courriels pour chaque domaine ou réseau				
11	Autorisations ou droits propriétaires pour les utilisateurs, les fichiers, les dossiers, les réseaux, les appareils				
12	Active Directory (AD), protocole allégé d'accès annuaire (LDAP), X.500 Statut d'enregistrement				
13	Date de la dernière vérification ou inspection ou du dernier examen				
14	Accès ou emplacement des rapports de données de l'utilisateur				

ANNEXE E: EXIGENCES RELATIVES À LA SÉCURITÉ

1.0 EXIGENCES RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEUR CANADIEN Nº DE DOSSIER DE PSPC: W636917DE25 et W636917DE26 – PHASE 1

1. **Le fournisseur / l'intimé** doit détenir en permanence, pendant l'exécution de cette **demande de renseignements,** une cote de sécurité d'installation valable au niveau **SECRET**, ainsi qu'une cote de protection des documents approuvée au niveau **SECRET,** délivrées par la Direction de la sécurité industrielle canadienne (CISD) de Travaux publics et Services gouvernementaux Canada (TPSGC).

2. **Cette demande de renseignements** comprend un accès à des marchandises contrôlées. Avant d'avoir accès, **le fournisseur / l'intimé** doit être inscrit au Programme des Marchandises Contrôlées de Travaux Publics et Services Gouvernementaux Canada

3. Les membres du personnel **du fournisseur / l'intimé** devant avoir accès à des renseignements ou à des biens CLASSIFIÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau **SECRET**, délivrée ou approuvée par la Direction de la DSIC de TPSGC.

4. Les membres du personnel **du fournisseur / l'intimé** devant avoir accès à des renseignements ou à des biens **RESTREINTE CLASSIFIÉS** ou à des établissements de travail dont l'accès est réglementé **doivent être citoyens du Canada, des États-Unis, du Royaume-Uni ou l'Australie** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau **SECRET**, délivrée ou approuvée par la DSIC de TPSGC.

5. Le traitement électronique de données CLASSIFIÉS dans l'établissement du **fournisseur / l'intimé,** n'est PAS autorisé dans le cadre de cette **demande de renseignements.**

6. L'entrepreneur ou l'offrant doit respecter les dispositions :

   a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu)

   b) du *Manuel de la sécurité industrielle* (dernière édition).

2.0 EXIGENCES RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEUR INTERNATIONAL Nº DE DOSSIER DE PSPC: W636917DE25 et W636917DE26 – PHASE 1

PROTÉGÉ A, PROTÉGÉ B, Confidentiel, Secret,

L'entrepreneur et les sous-traitants doivent être dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational, ou qui possèderont un tel instrument avec le Canada avant la fin de la période de soumission. Le programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de SPAC: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html

Tous les renseignements et les biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** fournis **au fournisseur / l'intimé** étranger destinataire doivent être protégés comme suit:

1. **Le fournisseur / l'intimé** étranger destinataire doit, en tout temps durant l'exécution de cette **demande de renseignements**, détenir une Attestation de sécurité d'installation valide, délivrée par l'autorité nationale de la sécurité (ANS) ou l'autorité désignée en matière de sécurité (ADS) **du pays du fournisseur / l'intimé**, d'un niveau équivalent à **SECRET**, et posséder une Cote de protection de documents de niveau **SECRET.**

2. Dans l'éventualité du retrait de la partie destinataire ou à la fin de cette **demande de renseignements**, tous les renseignements et les biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** fournis ou produits en vertu de cette **demande de renseignements** continueront d'être protégés, conformément aux politiques nationales **du pays du fournisseur / l'intimé**.

3. **Le fournisseur / l'intimé** étranger destinataire assurera une protection des renseignements et des biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'administration nationale de sécurité (ANS) ou par l'administration désignée en matière de sécurité (ADS) du pays du fournisseurs.

4. **Le fournisseur / l'intimé** étranger destinataire doit attribuer à tous les renseignements et biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** qui lui sont fournis par le gouvernement du Canada en vertu de cette **demande de renseignements** la cote de sécurité équivalente utilisée **par pays du fournisseur / l'intimé**, conformément aux politiques nationales **du pays du fournisseur / l'intimé.**

5. **Le fournisseur / l'intimé** étranger destinataire doit, en tout temps durant l'exécution de cette **demande de renseignements** veiller à ce que le transfert des renseignements et des biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** soit effectué conformément aux politiques nationales **du pays du fournisseur / l'intimé** et aux dispositions du Protocole d'entente bilatérale sur la sécurité industrielle signé par **le pays du fournisseur / l'intimé** et le Canada.

6. À la fin des travaux, **le fournisseur / l'intimé** étranger destinataire doit restituer au gouvernement du Canada, par l'entremise des circuits officiels, tous les renseignements et les biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** qu'il aura reçu ou produit en vertu de cette **demande de renseignements**, y compris tous les renseignements et les biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** remis à ses sous-traitants ou produits par eux.

7. Pour la durée de cette **demande de renseignements**, **le fournisseur / l'intimé** étranger destinataire doit se conformer aux politiques de son pays concernant l'examen, la possession ou le transfert de marchandises

contrôlées canadiennes. De plus, il doit immédiatement signaler à son administration nationale de la sécurité (ANS) tous les cas dans lesquels il sait ou a lieu de croire que des marchandises contrôlées fournies ou produites en vertu de cette **demande de renseignements** ont été perdus ou divulgués à des personnes non autorisées, notamment à une tiers entité, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants. La perte ou la compromission de marchandises contrôlées canadiennes lors de leur traitement à l'extérieur du Canada devrait être signalée immédiatement à l'autorité gouvernementale canadienne propriétaire des marchandises contrôlées canadiennes, par exemple le ministère canadien qui a émis les marchandises contrôlées canadiennes **au fournisseur / l'intimé** étranger bénéficiaire, dans le cadre de son **contrat / l'offre à commandes / contrat de sous-traitance**. La *Loi sur la production de défense* (LPD) définit le terme « marchandises contrôlées » (S.35)

8. **La demande de renseignements** prévoit l'accès à des données militaires non classifiées régies par les dispositions du *Règlement sur le contrôle des données techniques*. **Le fournisseur / l'intimé** américain destinataire doit devenir un entrepreneur agréé en vertu du Programme mixte d'agrément (PMA) États-Unis/Canada.

9. Les renseignements et les biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** doivent être divulgués uniquement aux membres du personnel employés par le destinataire étranger dans le cadre de cette **demande de renseignements** qui en ont besoin pour exécuter cette **demande de renseignements**. Ces membres du personnel doivent être des citoyens **de l'AUSTRALIE, du Royaume-Uni, des États-Unis d'Amérique**, et/ou un citoyen canadien et / ou un résident permanent du Canada, et doivent tous être titulaires d'une Attestation de sécurité du personnel valide de niveau **SECRET** exigée, délivrée ou approuvée par l'administration nationale de sécurité (ANS) ou par l'administration désignée en matière de sécurité (ADS) de leur pays respectif, conformément aux politiques nationales **du pays du fournisseur.**

10. Les renseignements/biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** fournis ou produits dans le cadre de cette **demande de renseignements** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:

    a. l'administration nationale de la sécurité (ANS) ou l'administration désignée en matière de sécurité (ADS) de l'autre sous-traitant étranger destinataire atteste par écrit que ce dernier a obtenu l'approbation d'accès aux renseignements/biens de niveau **NATO, étranger et CANADA PROTÉGÉ/CLASSIFIÉ** par l'intermédiaire de son ANS ou de son ADS;

    b. l'ANS ou l'ADS du pays du fournisseur donne son autorisation écrite lorsque l'autre sous-traitant destinataire étranger est situé dans un autre pays.

11. **Le fournisseur / l'intimé** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou conserver dans un système informatique des renseignements/biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** avant que l'administration nationale de la sécurité (ANS) ou l'administration désignée en matière de sécurité (ADS) du pays du fournisseurs lui en donne le droit. Une fois que **le fournisseur / l'intimé** étranger destinataire a reçu cette approbation écrite, il peut effectuer ces tâches jusqu'au niveau **SECRET**.

12. **Le fournisseur / l'intimé** étranger destinataire ne doit pas utiliser les renseignements /biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** pour répondre à des besoins distincts de l'exécution de cette **demande de renseignements** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être

obtenue auprès de l'ADS du Canada.

13. **Le fournisseur / l'intimé** étranger destinataire visitant des sites gouvernementaux ou industriels canadiens dans le cadre du contrat doit soumettre une demande de visite à l'administration désignée en matière de sécurité (ADS) du Canada, par l'entremise de son administration nationale de la sécurité (ANS) ou son administration désignée en matière de sécurité (ADS).

14. **Le fournisseur / l'intimé** étranger destinataire doit signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait ou il a lieu de croire que des renseignements/biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** obtenus dans le cadre de cette **demande de renseignements** ont été compromis.

15. **Le fournisseur / l'intimé** étranger destinataire doit immédiatement signaler à son administration nationale de la sécurité (ANS) ou à son administration désignée en matière de sécurité (ADS) tous les cas dans lesquels il sait où il a lieu de croire que des renseignements /biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** fournis ou produits par l**e fournisseur / l'intimé** étranger destinataire conformément à la **demande de renseignements** ont été perdus ou divulgués à des personnes non autorisées.

16. **Le fournisseur / l'intimé** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'intermédiaire de l'administration nationale de la sécurité (ANS) ou de l'administration désignée en matière de sécurité (ADS) du destinataire / ADS du Canada.

17. **Le fournisseur / l'intimé** étranger destinataire doit respecter les dispositions énoncées dans le protocole d'entente bilatéral en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational conclu entre **le pays du fournisseur** et le Canada pour déterminer les niveaux d'équivalence.

18. **Le fournisseur / l'intimé** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité.

19. Si un **fournisseur / intimé** étranger destinataire est choisi comme fournisseur dans le cadre de ce contrat, des clauses de sécurité propres a son pays seront établies et mises on œuvre 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.

ANNEXE F: APPLICATION DE LA POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (RIT).

Application de la Politique des retombées industrielles et technologiques

Le gouvernement du Canada envisage d'appliquer la Politique des retombées industrielles et technologiques (RIT) au projet **Sensibilisation à la cybersécurité** et au projet **Aide à la décision pour les cyberopérations défensives**. L'engagement avec l'industrie au moyen de la demande d'information permettra de déterminer l'application de la Politique des RIT et la façon dont le Canada peut tirer parti de ces approvisionnements dans un intérêt économique.

La politique des RIT, y compris la proposition de valeur

En vertu de la Politique des RIT, les entreprises qui se voient attribuer des contrats d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada, dont la valeur équivaut à celle du contrat. La Politique des RIT encourage les entreprises à faire des investissements à long terme au Canada, en les encourageant à s'établir ou à accroître leur présence au pays, en renforçant leurs chaînes d'approvisionnement ainsi qu'en développant des capacités industrielles canadiennes.

La Politique des RIT exige des soumissionnaires qu'ils se fassent concurrence sur la base des retombées économiques qu'ils pourraient offrir au Canada, et ce à travers la proposition de valeur associé à chaque soumission. Les soumissionnaires retenus sont sélectionnés en fonction du prix, du mérite technique et de la proposition de valeur. Après l'attribution du contrat, l'entrepreneur est tenu de s'acquitter de ses obligations en matière de RIT et de respecter les engagements pris dans le cadre de la proposition de valeur.

La Politique des RIT, y compris la proposition de valeur vise à soutenir la viabilité à long terme et la croissance du secteur de la défense au Canada, à améliorer la compétitivité et la croissance des fournisseurs canadiens, y compris les petites et moyennes entreprises, à investir dans la recherche et le développement de technologies au Canada ainsi qu'à favoriser ou à accroître l'accès aux marchés mondiaux et les exportations de biens et services du Canada. La Politique des RIT offre la possibilité de cibler d'autres secteurs d'investissement en fonction de chaque approvisionnement.

Pour obtenir plus d'information sur la Politique des RIT, y compris la proposition de valeur, veuillez vous rendre à l'adresse : www.canada.ca/rit

Secteur de la défense :

La Politique des RIT vise à promouvoir le développement économique et la viabilité à long terme des entreprises canadiennes chargées de la fabrication et de la prestation de produits et de services aux fins d'utilisation dans les applications de défense et de sécurité du gouvernement.

1. Quelles capacités canadiennes pourraient être utilisées pour soutenir directement la production et l'entretien de la plateforme aux projets Sensibilisation à la cybersécurité et Aide à la décision pour les cyberopérations défensives?

2. Quel pourcentage de travail direct lié aux projets Sensibilisation à la cybersécurité et Aide à la décision pour les cyberopérations défensives peut être réalisé au Canada?

Pour les définitions de la Politique des RIT, veuillez vous rendre à

l'adresse http://www.ic.gc.ca/eic/site/086.nsf/fra/h_00011.html.

Développement des sources d'approvisionnement, y compris les petites et moyennes entreprises:

La Politique des RIT cherche à rendre l'industrie canadienne plus concurrentielle, indépendamment de l'entrepreneur ou du donateur éligible, en renforçant la productivité, le perfectionnement des compétences et la capacité de relever les défis du marché.

1. Le secteur canadien de la cybersécurité compte près de 1 000 entreprises, la plupart des PME. Quelles opportunités de partenariats existe-t-il avec des PME canadiennes de moins de 250 employés afin d'effectuer des travaux directement liés aux projets Sensibilisation à la cybersécurité et Aide à la décision pour les cyberopérations défensives?

2. Quels types d'investissements le Canada devrait-il favoriser pour fournir aux entreprises canadiennes le plus de retombées possible dans le marché de la cybersécurité (secteur de la défense ou commercial)?

    a) Exemples

        (i) Création d'initiatives de formation et de développement de compétences afin d'attirer des travailleurs qualifiés et de les retenir (p. ex., codage et programmation, ingénierie des réseaux ainsi que développement et intégration de logiciels).

        (ii) Investissements dans de nouveaux biens d'équipement et de nouvelles ressources.

        (iii) Soutien en matière d'attestations de sécurité (p. ex., cote « Très secret » et ITAR) pour les entreprises canadiennes, surtout les petites et moyennes entreprises (PME).

3. La Politique des RIT exige qu'au moins 15 pour cent de l'obligation de l'entrepreneur relativement aux RIT (valeur équivalant à celle du contrat) corresponde à des travaux menés en collaboration avec des PME canadiennes comptant moins de 250 employés. Dans quelle mesure pouvez-vous satisfaire à une telle exigence imposée aux PME pour favoriser le développement de PME canadiennes dans le secteur de la cybersécurité (tant pour ce qui est du travail direct lié à ces approvisionnements qu'au travail mené dans d'autres secteurs d'activités)?

4. Mis à part ces approvisionnements, dans quels autres secteurs de production et de prestation de services entrevoyez-vous une possibilité d'aider les PME du secteur de la cybersécurité à prendre de l'expansion afin de répondre à la demande au pays et à l'étranger?

Recherche et développement (R-D):

La Politique des RIT encourage la recherche scientifique qui explore le développement de nouveaux biens et services, de nouveaux intrants à la production et de nouvelles méthodes de production des biens et services, ou de nouvelles façons d'exploiter et de gérer des organismes.

1. Existe-t-il des opportunités de partenariats avec des établissements post-secondaires canadiens ou des institutions de recherche financées par des fonds publics afin d'effectuer des travaux directement liés aux projets Sensibilisation à la cybersécurité et Aide à la décision pour les cyberopérations défensives?

2. Quels investissements de grande valeur en R-D réalisés au Canada, dans le secteur de la défense ou commercial, le Canada pourrait-il inciter les soumissionnaires à réaliser grâce à ces approvisionnements (p. ex., sécurité infonuagique, sécurité des appareils mobiles ou analyse de la sécurité)?

    a) Comment pourrait-on encourager les investissements dans les nouvelles technologies intersectorielles où le Canada offre des capacités (p. ex., l'informatique quantique, la réalité amplifiée/virtuelle ou l'intelligence artificielle/l'apprentissage machine)?

3. Pourrait-on créer des consortiums de recherche ou des centres d'excellence en partenariat avec des établissements d'études postsecondaires du Canada ou des établissements de recherche subventionnés par l'État ? Si c'est le cas, quels domaines de recherche votre entreprise pourrait-elle couvrir?

    a) Si non, quels autres partenariats en recherche ou en développement pourraient être créés pour soutenir le développement dans les domaines liés aux projets Sensibilisation à la cybersécurité et Aide à la décision pour les cyberopérations défensives?

4. Est-il possible d'investir dans des partenariats de recherche et développement avec des PME et des entreprises en démarrage canadiennes du secteur de la cybersécurité, y compris pour le financement des dernières étapes de la recherche et développement ainsi que la commercialisation de produits et de services novateurs?

5. Quelle devrait être l'exigence minimale en matière de R-D (pourcentage du prix de soumission prévu) pour inciter les soumissionnaires à investir dans l'innovation à valeur élevée dans le secteur de la cybersécurité canadien?

Exportation:

La Politique des RIT favorise la capacité des entreprises canadiennes et des PME à exploiter avec succès les marchés d'exportation, ce qui accroît leur productivité et compétitivité dans les marchés mondiaux.

1. Quelles sont les possibilités d'exportation du Canada liées directement à ces approvisionnements?

2. Est-il réalisable de détenir suffisamment de droits de propriété intellectuelle et d'obtenir un mandat de production mondiale exclusif vous permettant d'exporter vos opérations à partir du Canada, y compris les filiales et les partenaires de la chaîne d'approvisionnement?

3. Veuillez décrire les possibilités d'exportation de grande valeur à partir du Canada concernant des applications de cybersécurité générales, tant dans le secteur commercial que celui de la défense, pouvant être exploitées grâce à ces approvisionnements.

Questions additionnelles:

1. Comparativement au prix et au mérite technique, la proposition de valeur a généralement une pondération de 10 % de la note globale de la soumission. Que pensez-vous de la pondération de la proposition de valeur pour le projet Sensibilisation à la cybersécurité et le projet Aide à la décision pour les cyberopérations défensives?

2. Dans la proposition de valeur, quels pourcentages minimums de pondération recommandez-vous pour chacun des volets de la proposition de valeur (défense, développement des sources d'approvisionnement, R-D et exportation, et autres s'il y a lieu)?

Veuillez remettre vos réponses écrites et tout commentaire lié aux retombées industrielles et technologiques ou à la proposition de valeur à l’autorité contractante de Services publics et Approvisionnement Canada (SPAC) d’ici l’échéance de la demande de renseignements

ANNEXE G:RÈGLES D'ENGAGEMENT

1. Introduction

Ces règles d'engagement s'appliquent à l'ensemble du processus d'engagement et en particulier aux rencontres individuelles.

2. Règles et principes généraux

2.1. Un des principes fondamentaux de l'engagement de l'industrie est que le processus soit réalisé avec le plus haut degré de justice et d'équité entre toutes les parties. Nulle personne ou organisation ne doit recevoir ni sembler avoir reçu un quelconque avantage inhabituel ou injuste par rapport aux autres.

2.2. Les présentes règles d'engagement précoce entreront en vigueur à la signature de ce document, et prendront fin au moment de la publication de la demande de propositions.

2.3. Le processus d'engagement comprendra la demande de renseignement, les rencontres individuelles, une éventuelle ébauche de DP et tout autre processus jugé nécessaire par le responsable de l'approvisionnement.

2.4. Afin de maximiser les avantages du processus d'engagement, le Canada peut s'efforcer de solliciter les commentaires des participants sur diverses questions soulevées.

2.5. Les rencontres individuelles ne sont disponibles que pour les participants qui satisfont aux exigences de sécurité.

2.6. Les informations classifiées ne peuvent être divulguées qu'aux participants qui satisfont aux exigences de sécurité.

2.7. Les solutions, les idées ou les questions soulevées au cours des rencontres individuelles feront l'objet d'un examen plus poussé par le Canada.

2.8. Une version préliminaire de la DP pour examen définitif avant la publication officielle de la DP peut être mise à la disposition des participants qui satisfont aux exigences de sécurité.

2.9. Le Canada ne divulguera pas de renseignements exclusifs ou délicats sur le plan commercial concernant un participant à d'autres participants ou à des tiers, sauf dans la mesure où la loi l'exige.

2.10. Les répondants éventuels sont informés que tout renseignement soumis au Canada dans le processus d'engagement peut être utilisé par le Canada dans l'élaboration d'une demande de propositions concurrentielle.

3. Modalités

Les modalités suivantes s'appliquent au processus d'engagement. Afin de favoriser le dialogue, les participants acceptent ce qui suit :

3.1. Les participants doivent exposer leurs points de vue quant à l'approvisionnement et fournir des solutions positives aux problèmes soulevés. Tous les participants intéressés qui satisfont aux exigences de sécurité auront les mêmes chances de partager leurs idées et leurs suggestions.

3.2. Aucun enregistrement audio ou visuel ne sera autorisé pendant les rencontres individuelles.

3.3. Les participants doivent prévenir le Canada s'ils prévoient être accompagnés d'un avocat au moment de la rencontre individuelle. Le Canada se réserve le droit de refuser toute réunion en présence d'un avocat.

3.4. Les participants NE révéleront PAS ou ne discuteront d'aucune information sur les MÉDIAS ou dans les JOURNAUX quant à cette exigence au cours du processus d'engagement. Si les participants sont interrogés par les médias, ils doivent les orienter vers le Bureau des relations avec les médias de SPAC au 819-956-2313.

3.5. Les participants doivent présenter leurs questions et leurs commentaires UNIQUEMENT à l'autorité contractante de SPAC ou aux représentants autorisés du Canada, conformément aux indications données par l'autorité contractante. Toute communication avec des représentants non autorisés du Canada peut faire l'objet d'une divulgation complète par le Canada sur Achatsetventes.gc.ca.

3.6. Les médias ne peuvent participer au processus. Les médias doivent présenter leurs questions au Bureau des relations avec les médias de SPAC.

3.7. Le Canada n'est pas tenu d'émettre une DP ou de négocier un contrat pour les projets.

3.8. S'il publie une DP, le Canada doit en établir, à son gré, toutes les modalités.

3.9. Le Canada ne remboursera aucune personne ou entité pour tout coût engagé pour la participation à ce processus d'engagement de l'industrie.

3.10. La participation n'est pas obligatoire. Ne pas participer à ce processus n'empêche pas le soumissionnaire de soumettre une proposition lorsque la DP finale sera publiée.

3.11. La documentation préliminaire (DP, plan d'évaluation, EDT) sera diffusée aux participants qui satisfont aux exigences de sécurité pour obtenir leurs commentaires.

3.12. Les lobbyistes ne seront pas autorisés à participer au processus.

3.13. Dans le cadre de discussions informelles et de négociations de bonne foi, SPAC et le participant doivent faire tous les efforts raisonnables pour résoudre tout différend, toute controverse ou toute réclamation découlant de cet engagement de l'industrie, ou qui sont liés d'une quelconque façon à celui-ci.

ANNEXE H:INSCRIPTION POUR ASSISTER À LA RÉUNION DES REPRÉSENTANTS DE L'INDUSTRIE

Introduction

Tous les répondants de l'industrie intéressés sont invités à assister à une présentation de groupe non classifiée à l'intention de l'industrie, qui aura lieu dans la région de la capitale nationale, à Ottawa (Ontario), à la date indiquée au tableau 1 – Activité d'approvisionnement ou de consultation et dates connexes. La journée de l'industrie permettra au personnel du ministère de la Défense nationale qui est responsable du projet de donner un aperçu des deux projets, ainsi que d'obtenir les commentaires de l'industrie et de permettre à celle-ci de poser des questions à SPAC, au MDN et à ISDE. La journée de l'industrie se déroulera au niveau NON CLASSIFIÉ. Les fournisseurs qui ne participent pas à la journée de l'industrie peuvent tout de même soumettre une réponse à la présente RD.

Précisions sur la journée de l'industrie

Date: Le 26 février, 2018
Heure: 9 h -12h
Lieu : WOs&Sgts Mess, 4 Queen Elizabeth Dr., Ottawa

Date limite d'inscription : Le 16 février, 2018

Les fournisseurs sont priés d'arriver 30 minutes avant le mot d'ouverture de la journée de l'industrie afin de signer la feuille de présence.

Processus d'inscription

Les fournisseurs intéressés sont invités à s'inscrire à la journée de l'industrie au plus tard à la date limite d'inscription susmentionnée. Pour s'inscrire, les fournisseurs **doivent soumettre** les renseignements suivants à l'autorité contractante de SPAC indiquée ci-dessous :

- le nombre de personnes qui participeront à la journée de l'industrie;
- le nom et le titre professionnel de chaque participant;
- le courriel et le numéro de téléphone de la personne-ressource.

Veuillez prendre note de ce qui suit :

a. En raison du nombre limité de places, chaque fournisseur intéressé peut inscrire un maximum de deux (2) représentants pour assister à la journée de l'industrie.
b. Les noms de tous les participants peuvent être publiés après la journée de l'industrie.

En participant à la journée de l'industrie, aux séances individuelles et/ou à la réunion de suivi en groupe, les participants consentent à respecter les règles d'engagement énoncées à l'annexe G.

Le transport, l'hébergement, les repas, le stationnement et toute autre dépense sont aux frais des participants.

Autorité contractante pour la journée de l'industrie

Caroline Labrie
Services publics et Approvisionnement Canada
Place du Portage III, 8C2
11 Rue Laurier Gatineau, Quebec K1A 0S5
819-420-5725

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Il est préférable de communiquer par courriel

Présentation de renseignements avant la journée de l’industrie

Les fournisseurs peuvent soumettre des commentaires ou des questions par écrit, dans l’une des deux langues officielles, à l’autorité contractante dont le nom est indiqué ci-dessus.

Communication avec l’industrie

Le Canada mettra par écrit les préoccupations, les questions et les suggestions formulées lors de la journée de l’industrie, avec les réponses. Pendant le processus de consultation, l’autorité contractante de SPAC peut choisir de communiquer avec les participants de l’industrie inscrits par courriel plutôt que d’afficher d’autres avis sur le Service électronique d’appels d’offres du gouvernement (SEAOG). Pour assurer l’équité, la transparence et l’intégrité du processus, SPAC communiquera à l’industrie les renseignements découlant du processus (excluant les renseignements désignés exclusifs ou confidentiels).

L’exposé présenté par le Canada, les réponses aux questions soulevées au cours de la journée de l’industrie et la liste des participants seront publiés sur le Service électronique d’appels d’offres du gouvernement après la tenue de l’événement.

Langue

Tous les documents seront disponibles dans les deux langues officielles.

ANNEXE I: PRÉCISIONS SUR LES RENCONTRES INDIVIDUELLES ET LA RÉUNION DE SUIVI EN GROUPE ET INSCRIPTION

Introduction

L'intention des rencontres individuelles et de la séance de suivi en groupe est de distribuer et de présenter l'annexe C, ainsi que de tenir des discussions classifiées. L'annexe C donne un aperçu du concept actuel des opérations et des capacités en service, et elle est classifiée. La réunion de suivi en groupe sera tenue pour présenter et distribuer les questions et réponses classifiées issues des rencontres individuelles. **Étant donné que des renseignements classifiés seront communiqués dans le cadre des rencontres individuelles et de la réunion de suivi en groupe, les participants qui partent avec ces renseignements doivent satisfaire aux exigences de sécurité énoncées à l'annexe E.** Les attestations de sécurité seront confirmées auprès de la Direction de la sécurité industrielle canadienne (DSIC), ou par l'entremise de la Direction de la sécurité industrielle internationale (DSII) dans le cas des fournisseurs étrangers lorsqu'ils s'inscriront.

Étant donné que l'annexe C nécessite la production de marchandises contrôlées ou l'accès à des marchandises contrôlées qui sont visées par la *Loi sur la production de défense,* L.R., 1985, ch. D-1, l'entrepreneur et tout sous-traitant sont avisés que, au Canada, seules les personnes inscrites, exemptées ou exclues en vertu du Programme des marchandises contrôlées (PMC) sont légalement autorisées à examiner, à posséder ou à transférer des marchandises contrôlées. L'entrepreneur trouvera des précisions sur la façon de s'inscrire au PMC à l'adresse : http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-fra.html

Les fournisseurs doivent savoir que, bien que les exigences du MDN soient décrites de façon plus détaillée dans l'annexe C et lors de sa présentation à la rencontre individuelle, cette annexe n'est pas requise pour présenter une réponse exhaustive à la DR. Les fournisseurs ne sont pas tenus de se présenter à une rencontre individuelle ou d'assister à la réunion de suivi en groupe. Les fournisseurs qui ne seront pas présents peuvent tout de même soumettre une réponse à la présente RD.

Précisions sur les rencontres individuelles

Date : Du 26 février, 2018 au 2 mars 2018
Heure : Périodes de 1 heure tout au long de la semaine, à compter du 26 février 2018
Lieu : Quartier général de la Défense nationale, 101 Colonel By Drive, Ottawa

Les fournisseurs sont priés d'arriver 30 minutes avant l'heure de leur rencontre afin de signer la feuille de présence.

Précisions sur la réunion de suivi en groupe

Date : La date sera annoncée à la journée de l'industrie.
Heure : À déterminer – la semaine 5 mars, 2018
Lieu : Quartier général de la Défense nationale, 101 Colonel By Drive, Ottawa

Les fournisseurs sont priés d'arriver 30 minutes avant la réunion de groupe afin de signer la feuille de présence.

Processus d'inscription

Les fournisseurs intéressés doivent s'inscrire aux rencontres individuelles au plus tard à la date limite d'inscription indiquée dans le Tableau 1 – Activité d'approvisionnement ou de consultation et dates connexes. Les rencontres individuelles et la réunion de suivi en groupe auront lieu dans une installation sécurisée du ministère de la Défense nationale dans la région de la capitale nationale. L'inscription aux rencontres individuelles se déroulera selon le principe du premier arrivé, premier servi; toutefois, la disponibilité du MDN et du fournisseur, la confirmation des attestations de sécurité, les demandes de visite, etc., affecteront le calendrier des dates de réunions. Comme les

réunions auront lieu dans une installation du ministère de la Défense nationale, une demande de permis de visite (DPV) est également requise.

Pour s'inscrire, les fournisseurs **doivent soumettre** les renseignements suivants à l'autorité contractante de SPAC indiquée ci-dessous :

- le nombre de personnes qui assisteront à la réunion;
- le nom, le titre professionnel et la citoyenneté de chaque participant;
- le courriel et le numéro de téléphone de la personne-ressource.
- le numéro d'inscription au PMC ou une preuve écrite de l'exemption ou de l'exclusion du soumissionnaire et de toute autre personne à laquelle celui-ci donnera accès au l'annexe C..
- Veuillez signer l'entente de non-divulgation de l'organisation et de l'individu selon la forme prévue dans la pièce jointe no 1 de cette annexe, puis la faire parvenir à l'autorité contractante.

Veuillez prendre note de ce qui suit :

a. D'autres renseignements personnels et sur l'entreprise seront requis pour confirmer les attestations de sécurité et remplir la demande de permis de visite (DPV) du MDN.
b. En raison du nombre limité de places, chaque fournisseur intéressé peut inscrire un maximum de quatre (4) représentants pour assister à la rencontre individuelle et un maximum de deux (2) fournisseurs pour assister à la réunion de suivi en groupe.
c. Les noms de tous les participants peuvent être publiés après la journée de l'industrie.

En participant à la journée de l'industrie, aux séances individuelles et/ou à la réunion de suivi en groupe, les participants consentent à respecter les règles d'engagement énoncées à l'annexe G.

À la suite de la confirmation de l'attestation de sécurité, l'autorité contractante communiquera avec le fournisseur pour confirmer le lieu, la date et l'heure de la réunion.

Le transport, l'hébergement, les repas, le stationnement et toute autre dépense sont aux frais des participants.

Processus de réception et de transport de l'annexe C et des questions et réponses classifiées

L'annexe C de la présente DR et les questions et réponses classifiées issues des rencontres individuelles comportent des renseignements classifiés qui peuvent uniquement être communiqués aux répondants qui satisfont aux exigences de sécurité décrites à l'annexe E. Une version imprimée de l'annexe C sera distribuée aux rencontres individuelles, et sur demande à la réunion de suivi en groupe. Une version imprimée des questions et réponses classifiées sera distribuée à la réunion de suivi en groupe.

Tel que cela a été mentionné précédemment, **avant** la réunion, les fournisseurs doivent consulter le Manuel de la sécurité industrielle pour connaître les lignes directrices sur la manutention de documents classifiés, puisqu'ils **doivent** se conformer aux exigences de sécurité énoncées dans ce manuel : https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-fra.html.

Si un fournisseur a l'intention de conserver et de transporter la version imprimée de l'annexe C et des questions et réponses classifiées, il doit en présenter la demande par écrit à l'autorité contractante désignée ci-dessous. L'autorité contractante fera participer le MDN, la Direction de la sécurité industrielle canadienne (DSIC) ou la Direction de la sécurité industrielle internationale (DSII) au traitement de la demande. Puisque le processus d'approbation peut durer un certain nombre de semaines, les fournisseurs doivent soumettre leur demande le plus tôt possible.

Autorité contractante pour les rencontres individuelles et la réunion de groupe

Patti Wight
Services publics et Approvisionnement Canada
Place du Portage III, 8C2
11 Rue Laurier, Gatineau, Quebec K1A 0S5
819-420-1757

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Il est préférable de communiquer par courriel

Communication avec l’industrie

Le Canada prendra note de toutes les préoccupations, questions, suggestions et réponses formulées dans le cadre des rencontres individuelles. Pendant le processus de consultation, l’autorité contractante de SPAC peut choisir de communiquer avec les participants de l’industrie inscrits par courriel plutôt que d’afficher d’autres avis sur le Service électronique d’appels d’offres du gouvernement (SEAOG). Pour assurer l’équité, la transparence et l’intégrité du processus, SPAC partagera avec l’industrie les renseignements découlant du processus (excluant les renseignements désignés exclusifs ou confidentiels).

Les réponses non classifiées aux questions non classifiées soulevées au cours des rencontres individuelles ainsi que la liste des participants seront publiées sur le Service électronique d’appels d’offres du gouvernement après la réunion de suivi en groupe.

Langue

Tous les documents seront disponibles dans les deux langues officielles.

PIÈCE JOINTE NO 1 - L’ENTENTE DE NON-DIVULGATION

ENTREPRISE

ENTENTE DE NON-DIVULGATION EN VUE DE LA PARTICIPATION AU PROCESSUS DE DEMANDE DE SOUMISSIONS

NUMÉROS DE DOSSIER DE TPSGC W636917DE25 et W636917DE26 — PHASE I

Dans le cadre du processus de demande de soumissions susmentionné (le « **processus de demande de soumissions** »), y compris le volet « demande de renseignements » (« **DDR** »), des renseignements et des renseignements contrôlés doivent être divulgués (comme définis ci-dessous) au destinataire par le Canada ou au nom de celui-ci. Comme le Canada doit fournir ces renseignements, le destinataire reconnaît et convient que :

1. Renseignements

(a) Au cours du processus de demande de soumissions, le Canada pourrait divulguer des renseignements au destinataire : (i) qui ne sont pas des renseignements contrôlés (comme il est défini ci-dessous); ou (ii) qui sont des renseignements qui, autrement, ne sont pas rendus publics par le Canada sans obligation de confidentialité ou de non-divulgation (collectivement, les « **renseignements** »).

(b) Le Canada divulgue les renseignements au destinataire dans le seul et unique but de permettre au destinataire de participer au processus de demande de soumissions et, si le destinataire le souhaite, de préparer et de présenter une offre au Canada, si le Canada recherche de telles offres (le « **but** »).

(c) Le destinataire est tenu de préserver la confidentialité des renseignements relatifs au processus de demande de soumissions qui lui sont divulgués par le Canada ou au nom de celui-ci.

(d) Toute divulgation de renseignements doit être fondée sur le « besoin de connaître » des employés ou des conseillers juridiques et financiers du destinataire, lesquels doivent avoir signé au préalable l'entente de non-divulgation à l'intention des particuliers de l'annexe A. Le destinataire ne doit pas divulguer de renseignements à toute autre personne, y compris à ses entrepreneurs et à ses sous-traitants, sans avoir préalablement obtenu le consentement écrit du Canada; le destinataire ne doit pas non plus divulguer publiquement ou permettre la divulgation publique de renseignements, en totalité ou en partie, peu importe le but ou la nature des renseignements. Le destinataire ne doit pas modifier, retirer ou entraver tout avis de confidentialité ou tout autre avis concernant les renseignements et doit reproduire en totalité tous ces avis et toutes ces remarques dans toute copie, tout extrait ou tout autre document où pourraient figurer ces renseignements.

(e) Le destinataire peut divulguer des renseignements lorsque la loi ou une ordonnance d'un tribunal compétent l'exige, mais seulement dans la mesure nécessaire en vue de se conformer à la loi ou à l'ordonnance en question et sous condition que le destinataire ait préalablement fourni un avis écrit au Canada afin que celui-ci puisse, à sa seule discrétion, obtenir une ordonnance de confidentialité ou l'équivalent. Le destinataire est tenu d'aviser la personne ou l'entité pertinente à qui les renseignements seront divulgués de la nature confidentielle des renseignements en question et doit demander un traitement confidentiel. Sous réserve de ce qui précède, le destinataire doit se conformer à toute demande raisonnable du Canada relativement à ces divulgations.

(f) À moins d'une permission contraire aux termes du paragraphe (g), le destinataire est tenu, dès la réception d'une demande écrite du Canada ou dès l'achèvement du but ou de tout processus de demande de soumission à cet égard, de retourner ou de détruire (selon les consignes du Canada) tous les renseignements en sa possession ou sous sa responsabilité qui ont été divulgués par le Canada ou au nom de celui-ci. Le destinataire est aussi tenu de s'assurer du retour ou de la destruction (selon les consignes du Canada) de tous les renseignements en la possession ou sous la responsabilité de toute personne à qui de ces renseignements ont été divulgués, à l'exception du conseiller juridique du destinataire qui est autorisé à conserver une copie des renseignements, dans la mesure nécessaire, afin de remplir ses fonctions et de répondre aux exigences professionnelles qui lui incombent. Pour l'application du présent paragraphe, la « destruction » englobe la suppression de tout renseignement sauvegardé dans un ordinateur ou dans tout autre système électronique.

(g) Si un contrat est attribué au destinataire après sa participation au processus de demande de soumissions, le destinataire est autorisé à conserver les renseignements, à condition de continuer à respecter la présente entente et les dispositions applicables du contrat subséquent.

2. **Renseignements contrôlés**

(a) On entend par renseignements contrôlés : (i) tout renseignement ou tout matériel considéré comme un bien contrôlé selon la *section « Liste des marchandises contrôlées »* de la *Loi sur la production de défense*; (ii) tout renseignement assujetti au Programme de la sécurité industrielle du Canada ou au Programme de sécurité des contrats, y compris les renseignements ou le matériel PROTÉGÉ/CLASSIFIÉ; ou (iii) tout renseignement ou tout matériel considéré comme un bien contrôlé selon la *Loi sur la production de défense* et assujetti au Programme de la sécurité industrielle du Canada ou au Programme de sécurité des contrats.

(b) Le destinataire reconnaît et convient que tout usage de renseignements contrôlés, notamment l'accès libre, la reproduction, la distribution, la divulgation, la transmission, la retransmission, l'exportation, la réexportation, l'acheminement, le réacheminement, la conservation et la destruction (ou l'interdiction de destruction) de renseignements contrôlés, doit être fondé sur le « besoin de connaître » pour le seul et unique but recherché, sous réserve de ce qui suit, le cas échéant : (i) le *Règlement sur les marchandises contrôlées* et les exigences de la Direction des marchandises contrôlées (y compris l'inscription, la conformité et l'exemption); et (ii) le Programme de la sécurité industrielle du Canada ou le Programme de sécurité des contrats, ou toute autre exigence prévue par de ces programmes, notamment les exigences relatives à la sécurité établies dans l'annexe B et l'annexe C (selon le cas) de la présente entente. Aucune disposition prévue par la présente entente ne limite les obligations du destinataire prévues dans le cadre des programmes susmentionnés et ne lui permet d'y déroger.

(c) Le destinataire convient que (i) le Canada peut divulguer des renseignements contrôlés au destinataire dans le cadre du processus de demande de soumissions, dans la mesure où le destinataire est autorisé à recevoir de tels renseignements contrôlés; et (ii) le destinataire peut ne pas être autorisé à recevoir tous les renseignements contrôlés qui devraient être divulgués par le Canada dans le cadre du processus de demande de soumissions. Il incombe au destinataire de s'assurer d'avoir l'ensemble des autorisations et des permissions requises en tout temps.

Sans limiter la portée de ce qui précède, le destinataire peut retourner ou détruire (à la seule et unique discrétion du Canada) tout renseignement contrôlé. Le destinataire convient que de telles directives peuvent être données par le Canada à sa seule et unique discrétion, peu importe si le processus de demande de soumissions est terminé ou annulé, ou si le but est achevé.

3. Généralités

(a) Le destinataire est responsable de l'ensemble des dommages, des coûts, des pertes et des dépenses qui découlent du non-respect de la présente entente de la part du destinataire, de ses employés, de ses représentants ou de toute autre partie à qui le destinataire divulgue des renseignements ou des renseignements contrôlés. Les dispositions prévues par la présente entente continuent de s'appliquer après la résiliation de l'entente, le retour ou la destruction de renseignements ou de renseignements contrôlés, l'achèvement du but et l'annulation ou l'achèvement du processus de demande de soumissions. La présente entente ainsi que tout conflit ou toute plainte découlant de celle-ci ou s'y rapportant doivent être appliqués et interprétés conformément aux lois de la province de l'Ontario

Nom du destinataire : _____

[Insérer la raison sociale (le nom légal)]

J'ai le pouvoir de lier le destinataire

Par : _____

Nom (en lettres moulées) : _____

Date : _____

Agent de sécurité du destinataire

Par : _____

Nom (en lettres moulées) : _____

Date : _____

ANNEXE A

PARTICULIER

ENTENTE DE NON-DIVULGATION EN VUE DE LA PARTICIPATION AU PROCESSUS DE DEMANDE DE SOUMISSIONS NUMÉROS DE DOSSIER DE TPSGC W636917DE25 et W636917DE26 — PHASE I

Dans le cadre du processus de demande de soumissions susmentionné (le « **processus de demande de soumissions** »), y compris le volet « demande de renseignements » (« **DDR** »), des renseignements et des renseignements contrôlés doivent être divulgués (comme définis ci-dessous) au destinataire au nom du Canada ou par son employeur (l'« **entreprise** »). Comme le Canada doit fournir ces renseignements, le destinataire reconnaît et convient que :

1. Renseignements

(a) Au cours du processus de demande de soumissions, certains renseignements pourraient être divulgués au destinataire par l'entreprise, par le Canada ou au nom du Canada, soit des renseignements : (i) qui ne sont pas des renseignements contrôlés (comme il est défini ci-dessous); ou (ii) qui, autrement, ne sont pas rendus publics par le Canada sans obligation de confidentialité ou de non-divulgation (collectivement, les « **renseignements** »).

(b) Les renseignements sont divulgués au destinataire dans le seul et unique but de permettre au destinataire de participer au processus de demande de soumissions sous la direction et au nom de l'entreprise (le « **but** »).

(c) Le destinataire est tenu de préserver la confidentialité de l'ensemble des renseignements qui lui sont divulgués. Toute divulgation de renseignements doit être fondée sur le « besoin de connaître » des employés de l'entreprise qui sont autorisés par l'entreprise à recevoir ces renseignements. Le destinataire ne doit pas divulguer de renseignements à toute autre personne, y compris aux entrepreneurs et aux sous-traitants de l'entreprise, sans avoir préalablement obtenu le consentement écrit de l'entreprise; le destinataire ne doit pas non plus divulguer publiquement ou permettre la divulgation publique de renseignements, en totalité ou en partie, peu importe le but ou la nature des renseignements. Le destinataire ne doit pas modifier, retirer ou entraver tout avis de confidentialité ou tout autre avis concernant les renseignements et doit reproduire en totalité tous ces avis et toutes ces remarques dans toute copie, tout extrait ou tout autre document où pourraient figurer ces renseignements.

(d) Le destinataire peut divulguer des renseignements si l'entreprise lui confirme que la loi ou une ordonnance d'un tribunal compétent l'exige, mais seulement dans la mesure nécessaire en vue de se conformer à la loi ou à l'ordonnance en question et à condition que le destinataire, sous toutes réserves, respecte l'ensemble des directives de l'entreprise relativement à la présente disposition.

(e) Le destinataire est tenu, à la demande de l'entreprise, de retourner ou de détruire tous les renseignements en sa possession ou sous sa responsabilité. Pour l'application du présent paragraphe, la « destruction » englobe la suppression de tout renseignement sauvegardé dans un ordinateur ou dans tout autre système électronique.

2. Renseignements contrôlés

(a) Controlled Information means: (i) any information or materials that are a controlled good as defined in *Schedule (Controlled Goods List)* of the *Defence Production Act*, or (ii) any information that is subject to Canada's Industrial or Contract Security Program, including PROTECTED/CLASSIFIED information or materials; or (iii) information or materials that are both a controlled good as defined in the *Defence Production Act* and subject to Canada's Industrial or Contract Security Program.

(b) Any and all use of Controlled Information, including without limitation, all access, copying, distribution, disclosure, transmission, retransmission, export, re-export, transfer, re-transfer, storage and destruction (or prohibitions on destruction) of Controlled Information, shall be on a "need to know" basis solely and exclusively for the Purpose and shall be subject to and in compliance with, as applicable: (i) the *Controlled Goods Regulations* and the requirements of the Controlled Goods Program (including registration, compliance, or exemption); and (ii) Canada's Industrial or Contract Security Program including any Security Agreement or other requirements of such Program(s), including those Security Requirements as set forth in Annexes B and C (as applicable) to this Agreement. Nothing contained in this Agreement limits or otherwise derogates from Recipient's obligations under either of the foregoing Programs.

(c) Without limiting the foregoing, Recipient shall immediately, at Company's direction, return or destroy any Controlled Information in Recipient's possession or under Recipient's control.

3. Généralités

(a) Le destinataire est tenu d'aviser l'entreprise de toute violation de la présente entente. Les dispositions prévues par la présente entente continuent de s'appliquer après la résiliation de l'entente, le retour ou la destruction de renseignements ou de renseignements contrôlés, l'achèvement du but et l'annulation ou l'achèvement du processus de demande de soumissions. La présente entente ainsi que tout conflit ou toute plainte découlant de celle-ci ou s'y rapportant doivent être appliqués et interprétés conformément aux lois de la province de l'Ontario

Entreprise (en lettres moulées) : _____ **Destinataire (en lettres moulées) :** _____ Signature : _____ Date : _____	**Agent de sécurité de l'entreprise (en lettres moulées)** : _____ Signature : _____ Date : _____

ANNEXE B

No de dossier de PSPC W636917DE25 et W636917DE26 – PHASE I pour les fournisseur Canadien

1. **Le fournisseur / l'intimé** doit détenir en permanence, pendant l'exécution de cette **demande de renseignements**, une cote de sécurité d'installation valable au niveau SECRET, ainsi qu'une cote de protection des documents approuvée au niveau SECRET, délivrées par la Direction de la sécurité industrielle canadienne (CISD) de Travaux publics et Services gouvernementaux Canada (TPSGC).

2. Cette **demande de renseignements** comprend un accès à des marchandises contrôlées. Avant d'avoir accès, le **fournisseur / l'intimé** doit être inscrit au Programme des Marchandises Contrôlées de Travaux Publics et Services Gouvernementaux Canada

3. Les membres du personnel du **fournisseur / l'intimé** devant avoir accès à des renseignements ou à des biens CLASSIFIÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, délivrée ou approuvée par la Direction de la DSIC de TPSGC.

4. Les membres du personnel du **fournisseur / l'intimé** devant avoir accès à des renseignements ou à des biens RESTREINTE CLASSIFIÉS ou à des établissements de travail dont l'accès est réglementé doivent être citoyens du Canada, des États-Unis, du Royaume-Uni ou l'Australie et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, délivrée ou approuvée par la DSIC de TPSGC.

5. Le traitement électronique de données CLASSIFIÉS dans l'établissement du **fournisseur / l'intimé**, n'est PAS autorisé dans le cadre de cette **demande de renseignements.**

6. L'entrepreneur ou l'offrant doit respecter les dispositions :

   a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu)
   b) du Manuel de la sécurité industrielle (dernière édition).

ANNEX C

PWGSC FILE#'s W636917DE25 and W636917DE26 – PHASE I for International suppliers

PROTÉGÉ A, PROTÉGÉ B, Confidentiel, Secret,

Le fournisseur / l'intimé doivent être dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational, ou qui possèderont un tel instrument avec le Canada avant la fin de la période de soumission. Le programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de SPAC: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html

Tous les renseignements et les biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** fournis **au fournisseur / l'intimé** étranger destinataire doivent être protégés comme suit:

1. **Le fournisseur / l'intimé** étranger destinataire doit, en tout temps durant l'exécution de cette **demande de renseignements**, détenir une Attestation de sécurité d'installation valide, délivrée par l'autorité nationale de la sécurité (ANS) ou l'autorité désignée en matière de sécurité (ADS) **du pays du fournisseur / l'intimé**, d'un niveau équivalent à **SECRET**, et posséder une Cote de protection de documents de niveau **SECRET.**
2. Dans l'éventualité du retrait de la partie destinataire ou à la fin de cette **demande de renseignements**, tous les renseignements et les biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** fournis ou produits en vertu de cette **demande de renseignements** continueront d'être protégés, conformément aux politiques nationales **du pays du fournisseur / l'intimé**.
3. **Le fournisseur / l'intimé** étranger destinataire assurera une protection des renseignements et des biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'administration nationale de sécurité (ANS) ou par l'administration désignée en matière de sécurité (ADS) du pays du fournisseurs.
4. **Le fournisseur / l'intimé** étranger destinataire doit attribuer à tous les renseignements et biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** qui lui sont fournis par le gouvernement du Canada en vertu de cette **demande de renseignements** la cote de sécurité équivalente utilisée **par pays du fournisseur / l'intimé**, conformément aux politiques nationales **du pays du fournisseur / l'intimé.**
5. **Le fournisseur / l'intimé** étranger destinataire doit, en tout temps durant l'exécution de cette **demande de renseignements** veiller à ce que le transfert des renseignements et des biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** soit effectué conformément aux politiques nationales **du pays du fournisseur / l'intimé** et aux dispositions du Protocole d'entente bilatérale sur la sécurité industrielle signé par **le pays du fournisseur / l'intimé** et le Canada.
6. À la fin des travaux, **le fournisseur / l'intimé** étranger destinataire doit restituer au gouvernement du Canada, par l'entremise des circuits officiels, tous les renseignements et les biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** qu'il aura reçu ou produit en vertu de cette **demande de renseignements**, y compris tous les renseignements et les biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** remis à ses sous-traitants ou produits par eux.
7. Pour la durée de cette **demande de renseignements**, **le fournisseur / l'intimé** étranger destinataire doit se conformer aux politiques de son pays concernant l'examen, la possession ou le transfert de marchandises contrôlées canadiennes. De plus, il doit immédiatement signaler à son administration nationale de la sécurité (ANS) tous les cas dans lesquels il sait ou a lieu de croire que des marchandises contrôlées fournies ou produites en vertu de cette **demande de renseignements** ont été perdus ou divulgués à des personnes non autorisées, notamment à une tiers entité, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants. La perte ou la compromission de marchandises contrôlées canadiennes lors de leur traitement à l'extérieur du Canada devrait être signalée immédiatement à l'autorité gouvernementale canadienne propriétaire des marchandises contrôlées canadiennes, par exemple le ministère canadien qui a émis les marchandises contrôlées canadiennes **au fournisseur / l'intimé** étranger bénéficiaire, dans le cadre de son **contrat / l'offre à commandes / contrat de sous-traitance**. La *Loi sur la production de défense* (LPD) définit le terme « marchandises contrôlées » (S.35)
8. **La demande de renseignements** prévoit l'accès à des données militaires non classifiées régies par les dispositions du *Règlement sur le contrôle des données techniques*. **Le fournisseur / l'intimé** américain destinataire doit devenir un entrepreneur agréé en vertu du Programme mixte d'agrément (PMA) États-Unis/Canada.
9. Les renseignements et les biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** doivent être divulgués uniquement aux membres du personnel employés par le destinataire étranger dans le cadre de cette **demande de renseignements** qui en ont besoin pour exécuter cette **demande de renseignements**. Ces membres du personnel doivent être des citoyens **de l'AUSTRALIE, du Royaume-Uni, des États-Unis d'Amérique**, et/ou un citoyen canadien et / ou un résident permanent du Canada, et doivent tous être titulaires d'une Attestation de sécurité du personnel valide de niveau **SECRET** exigée, délivrée ou approuvée par l'administration nationale de sécurité (ANS) ou par l'administration désignée en matière de sécurité (ADS) de leur pays respectif, conformément aux politiques nationales **du pays du fournisseur.**
10. Les renseignements/biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** fournis ou produits dans le cadre de cette **demande de renseignements** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:

    a. l'administration nationale de la sécurité (ANS) ou l'administration désignée en matière de sécurité (ADS) de l'autre sous-traitant étranger

destinataire atteste par écrit que ce dernier a obtenu l'approbation d'accès aux renseignements/biens de niveau **NATO, étranger et CANADA PROTÉGÉ/CLASSIFIÉ** par l'intermédiaire de son ANS ou de son ADS;

b. l'ANS ou l'ADS du pays du fournisseur donne son autorisation écrite lorsque l'autre sous-traitant destinataire étranger est situé dans un autre pays.

11. **Le fournisseur / l'intimé** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou conserver dans un système informatique des renseignements/biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** avant que l'administration nationale de la sécurité (ANS) ou l'administration désignée en matière de sécurité (ADS) du pays du fournisseurs lui en donne le droit. Une fois que **le fournisseur / l'intimé** étranger destinataire a reçu cette approbation écrite, il peut effectuer ces tâches jusqu'au niveau **SECRET**.
12. **Le fournisseur / l'intimé** étranger destinataire ne doit pas utiliser les renseignements /biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** pour répondre à des besoins distincts de l'exécution de cette **demande de renseignements** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS du Canada.
13. **Le fournisseur / l'intimé** étranger destinataire visitant des sites gouvernementaux ou industriels canadiens dans le cadre du contrat doit soumettre une demande de visite à l'administration désignée en matière de sécurité (ADS) du Canada, par l'entremise de son administration nationale de la sécurité (ANS) ou son administration désignée en matière de sécurité (ADS).
14. **Le fournisseur / l'intimé** étranger destinataire doit signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait ou il a lieu de croire que des renseignements/biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** obtenus dans le cadre de cette **demande de renseignements** ont été compromis.
15. **Le fournisseur / l'intimé** étranger destinataire doit immédiatement signaler à son administration nationale de la sécurité (ANS) ou à son administration désignée en matière de sécurité (ADS) tous les cas dans lesquels il sait où il a lieu de croire que des renseignements /biens de niveau **CANADA PROTÉGÉ / CLASSIFIÉ** fournis ou produits par l**e fournisseur / l'intimé** étranger destinataire conformément à la **demande de renseignements** ont été perdus ou divulgués à des personnes non autorisées.
16. **Le fournisseur / l'intimé** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **CANADA PROTÉGÉ/CLASSIFIÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'intermédiaire de l'administration nationale de la sécurité (ANS) ou de l'administration désignée en matière de sécurité (ADS) du destinataire / ADS du Canada.
17. **Le fournisseur / l'intimé** étranger destinataire doit respecter les dispositions énoncées dans le protocole d'entente bilatéral en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational conclu entre **le pays du fournisseur** et le Canada pour déterminer les niveaux d'équivalence.
18. **Le fournisseur / l'intimé** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité.

Si un **fournisseur / intimé** étranger destinataire est choisi comme fournisseur dans le cadre de ce contrat, des clauses de sécurité propres a son pays seront établies et mises on œuvre 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.

ANNEXE J: DEMANDE DE PARRAINAGE POUR UNE ATTESTATION DE SÉCURITÉ

Introduction

Étant donné que la DR comprend une annexe classifiée, et puisque la version préliminaire de la DP, la DP finale et le contrat subséquent peuvent aussi contenir des renseignements classifiés, l'un des principaux objets de la présente DR consiste à fournir des directives et une assistance aux fournisseurs intéressés qui ne satisfont pas aux exigences de sécurité exposées en détail à l'annexe E afin qu'ils obtiennent l'attestation de sécurité requise.

Demande de parrainage pour les étapes 1 à 3 (de la DR à la DP)

Les fournisseurs dont les organisations ne détiennent actuellement pas une attestation de sécurité d'installation valide de niveau SECRET, non plus qu'une autorisation de détenir des documents de niveau SECRET délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de SPAC, sont invités à entreprendre immédiatement le processus d'attestation. Les demandes de parrainage peuvent être transmises par courriel à l'autorité contractante de SPAC indiquée ci-dessous.

Autorité contractante principale pour le parrainage en matière de sécurité

Caroline Labrie
Services publics et Approvisionnement Canada
Place du Portage III, 8C2
11 Rue Laurier Gatineau, Quebec K1A 0S5
819-420-5725
TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Il est préférable de communiquer par courriel.

Il incombe au fournisseur de veiller à ce que l'information relative aux attestations de sécurité soit fournie dans les délais prescrits à l'autorité compétente ou à la DSIC. La demande doit comprendre les renseignements suivants :

a) Dénomination sociale de l'entreprise :
b) Dénomination commerciale, si elle est différente de la dénomination sociale :
c) Adresse postale :
d) Adresse municipale, si elle est différente de l'adresse postale :
e) Numéro de téléphone de l'entreprise :
f) Numéro de télécopieur de l'entreprise :
g) Nom et prénom de la personne-ressource (représentant au Canada) :
h) Titre de la personne-ressource :
i) Numéro de téléphone de la personne-ressource :
j) Adresse courriel de la personne-ressource :
k) Langue de correspondance (français ou anglais) :

À la réception de la demande de parrainage, la DSIC communiquera avec le soumissionnaire éventuel pour achever la collecte des renseignements requis.

Pour toute demande de renseignements sur les exigences en matière de sécurité, le fournisseur doit communiquer avec la DSIC au 1-866-368-4646, ou au 613-948-4176 dans la région de la capitale nationale. Adresse du site Web de la DSIC : http://ssi-iss.tpsgc-pwgsc.gc.ca/index-fra.html.

Aucun coût direct n’est facturé aux fournisseurs qui souhaitent obtenir une attestation de sécurité d’installation (ASI). Toutefois, des coûts indirects, liés au besoin de respecter les normes minimales comme l’installation de mécanismes pour la protection des documents, peuvent s’appliquer.

Demande de parrainage pour l’étape 4 (attribution du contrat)

Étant donné que les exigences de sécurité pour l’étape 4 sont toujours en cours d’élaboration, SPAC **ne parraine actuellement pas** la délivrance des attestations mentionnées ci-après. Lorsque la version définitive des exigences de sécurité sera achevée, la DR peut être modifiée pour y inclure le parrainage des fournisseurs afin qu’ils obtiennent ces attestations.

Lors de l’attribution du contrat, le fournisseur sélectionné recevra l’accès à de l’information classifiée collectivement au niveau TRÈS SECRET (SIGINT) et qui n’est accessible qu’aux citoyens canadiens. À l’heure actuelle, on estime que l’entrepreneur principal sélectionné doit, à tout le moins, détenir les attestations de sécurité d’installation obligatoires suivantes :

1) Niveau TRÈS SECRET (SIGINT) pour le personnel assigné, limité au personnel détenant la citoyenneté canadienne;

2) Niveaux SECRET et OTAN SECRET pour la protection des documents, avec des exigences spécifiques en matière de sécurité de la technologie de l’information.