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 Sensibilisation à la cybersécurité	
Solicitation No. - N° de l'invitation W6369-17DE26/A	**Date** 2016-12-15
Client Reference No. - N° de référence du client W6369-17DE26	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-049-26099
File No. - N° de dossier 049qe.W6369-17DE26	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2017-01-26**	**Time Zone** **Fuseau horaire** Eastern Standard Time EST
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

Destination Code - Code destinataire	Destination Address - Adresse de la destination	Invoice Code - Code bur.-comptable	Invoice Address - Adresse de facturation
D - 1	DEPARTMENT OF NATIONAL DEFENCE WOODLINE BUILDING 2 CONSTELLATION Crescent OTTAWA, ON K2G 5J9	W6369	DEPARTMENT OF NATIONAL DEFENCE 101 COLONEL BY DR. Woodline Building OTTAWA Ontario K1A0K2 Canada

Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM Destination	Plant/Usine	Delivery Req. Livraison Req.	Del. Offered Liv. offerte
1	Letter of Interest (LOI) for CSA	D - 1	W6369	1	Each	$	XXXXXXXXXX	See Herein	

TABLE DES MATIÈRES

Objet et contenu de la présente lettre d'intérêt

Il s'agit de la lettre d'intérêt (LI) ayant trait à le project Sensibilisation à la cybersécurité pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). La lettre d'intérêt (LI) orientera et préparera l'industrie en vue d'éventuelles possibilités d'approvisionnement dans le cadre du projet Sensibilisation à la cybersécurité et vise à obtenir des commentaires et la contribution de l'industrie en ce qui a trait à la portée, aux exigences, au calendrier, aux risques et aux coûts éventuels du projet

Le contenu général de la présente LI est le suivant :

PARTIE I : Processus de lettre d'intérêt: Renseignements sur l'objet de la présente LI et la procédure que l'industrie doit suivre pour y répondre.

PARTIE II: Sensibilisation à la cybersécurité; Contexte; Objectifs; Exigences en matière de sécurité, Exception au titre de la sécurité nationale, Politique des retombées industrielles et technologiques (rit), De langues officielles et; Stratégie d'engagement

PARTIE III : Questions à l'intention de l'industrie : Questions qui visent à obtenir de la rétroaction de l'industrie et qui permettront au MDN/CAF de définir ses exigences techniques et la demande de soumissions.

ANNEXE A : Description généralisée d'un modèle d'infrastructure réseau
ANNEXE B : Environnements de mission et scénarios opérationnels
ANNEXE C : Exigences opérationnelles préliminaires
ANNEXE D : Méthode d'analyse de rentabilisation

PARTIE I : PROCESSUS DE LETTRE D'INTÉRÊT

1. INTRODUCTION

Il s'agit de la lettre d'intérêt (LI) ayant trait à le project Sensibilisation à la cybersécurité pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). La lettre d'intérêt (LI) orientera et préparera l'industrie en vue d'éventuelles possibilités d'approvisionnement dans le cadre du projet Sensibilisation à la cybersécurité et vise à obtenir des commentaires et la contribution de l'industrie en ce qui a trait à la portée, aux exigences, au calendrier, aux risques et aux coûts éventuels du projet.

Le projet Sensibilisation à la cybersécurité en est actuellement à la première phase d'analyse des options (AO), ce qui signifie que l'analyse de rentabilisation et la justification du projet sont en cours d'élaboration. Ainsi, aucune décision sur les concepts, les technologies ou les solutions n'a été prise. L'objectif de la phase d'AO est de veiller à ce que la haute direction du Ministère prenne une décision avisée sur la meilleure façon de définir le projet (c'est-à-dire, exécuter la phase de définition) et, s'il y a lieu, mettre en œuvre le projet pour atteindre la capacité requise.

L'objectif est de consulter activement l'industrie tout au long des phases d'AO et de définition pour assurer un état final du projet réussi. La rétroaction de l'industrie aidera l'équipe de projet du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) à définir :

a. l'énoncé des besoins opérationnels (EBO) de façon compréhensible pour l'industrie et sensée pour le contexte opérationnel du MDN et des FAC, afin de contribuer de façon subséquente à une meilleure description de la correspondance stratégique et des besoins opérationnels pour le MDN et les FAC;

b. « l'art du possible » concernant la capacité TI d'entreprise, les progrès au sein de l'industrie, la transformation de grandes sociétés semblables pour répondre à la technologie et aux besoins changeants – tout cela mène à une meilleure définition de l'EBO, du budget et du calendrier nécessaires pour répondre aux objectifs du projet (autant au niveau de la technologie que de l'industrie/l'approvisionnement);

c. l'incidence sur les personnes, les processus et les technologies de divers concepts proposés et les changements organisationnels qui seront nécessaires pour appuyer chacune des solutions conceptuelles;

d. la nature et les sources des coûts de projet, y compris le besoin de tâches de la phase de définition, les coûts de la phase de mise en œuvre et le soutien en service (SES) à long terme;

e. la stratégie d'approvisionnement la plus appropriée avec laquelle l'industrie est d'accord et qui fournit le bon équipement au bon moment, en mettant à profit les achats afin de créer des emplois et de stimuler la croissance au Canada, en plus de simplifier les processus d'approvisionnement.

Le MDN et les FAC ne communiqueront pas avec les fournisseurs à la suite de la présente lettre d'intérêt (LI). L'autorité contractante indiquée à la section 2.7 peut communiquer avec l'industrie pour obtenir plus de renseignements sur les réponses. Toute activité de consultation de l'industrie ou tout marché à venir sera publié.

1.1 Nature de la présente lettre d'intérêt

La présente LI ne constitue pas une demande de soumissions. Elle ne donnera pas lieu à l'attribution d'un contrat. Par conséquent, les fournisseurs éventuels de biens ou de services décrits dans la LI ne doivent pas réserver des stocks ou des installations ni affecter des ressources en fonction des renseignements présentés dans la LI. Cette dernière ne donnera pas lieu non plus à l'établissement d'une liste de fournisseurs. La participation de tout fournisseur éventuel à la présente LI n'empêche aucunement le fournisseur de participer à toute autre demande ultérieure. En outre, la présente LI n'entraînera pas nécessairement l'acquisition de l'un ou

l'autre des biens et des services qui y sont décrits. La LI vise seulement à obtenir des commentaires de l'industrie sur les éléments qui y sont présentés.

2. CONSIGNES À SUIVRE POUR RÉPONDRE À LA PRÉSENTE LETTRE D'INTÉRÊT

2.1 Nature et format des réponses demandées

La présente LI n'est pas une demande de soumissions. 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 d'atteindre les objectifs décrits dans la présente LI. Les répondants devraient expliquer toute hypothèse énoncée dans leurs réponses.

Les réponses ne serviront pas à des fins de concours ou d'évaluation comparative. Elles ne sont donc pas dans un format aussi rigide que le seraient les réponses à une DP; toutefois, dans le souci de recueillir des réponses qui seront faciles à traiter et qui auront la plus grande utilité, le gouvernement du Canada prie les répondants d'observer la structure décrite à la section 2.6.

2.2 Coûts associés aux réponses

Le Canada ne remboursera pas les dépenses que les organisations engageront pour répondre à la présente LI.

2.3 Traitement des réponses

Utilisation des réponses : Les réponses ne seront pas soumises à une évaluation formelle. Toutefois, le Canada pourra les utiliser afin d'élaborer ou de modifier la stratégie d'approvisionnement. Le Canada examinera, d'ici la date de la clôture de la LI, toutes les réponses reçues. Cependant, s'il le juge opportun, il pourrait également examiner des réponses reçues après la date de clôture de la LI.

Équipe d'examen : Une équipe d'examen, composée de représentants du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) et de Travaux publics et services gouvernementaux Canada (TPSGC), examinera les réponses reçues. Le Canada se réserve le droit d'embaucher des experts-conseils indépendants ou d'utiliser des ressources du gouvernement du Canada, s'il le juge nécessaire, pour l'examen des réponses. Chaque réponse ne sera pas nécessairement examinée par tous les membres de l'équipe d'examen.

Confidentialité : Chaque répondant devrait indiquer clairement chaque élément de sa réponse qu'il considère comme confidentiel ou de

2.4 Communication avec l'industrie

L'autorité contractante peut communiquer avec l'industrie pour obtenir plus de renseignements sur toute réponse.

2.5 Contenu de la demande de renseignements

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 exigences soient retirées ou modifiées. Les observations concernant cet aspect du document préliminaire sont les bienvenues. La présente LI contient également des questions précises à l'intention de l'industrie.

2.6 Format des réponses

Page couverture : Si la réponse comporte plusieurs volumes, les répondants sont priés d'indiquer sur la page couverture de chacun des volumes le titre de la réponse, le numéro de la demande, le numéro du volume et leur dénomination sociale complète.

Page titre : La première page suivant la page de couverture doit être une page titre. Celle-ci doit comporter les éléments suivants :

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

ii) Le nom et l'adresse du répondant;

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

iv) La date;

v) Le numéro de la LI.

Nombre d'exemplaires : Le Canada demande aux répondants de transmettre leur réponse dans un format PDF non protégé (c.-à-d. sans mot de passe) par courriel, si la taille du document est inférieure à 6 Mo, à l'adresse suivante :

patti.wight@tpsgc-pwgsc.gc.ca

Autrement, le Canada demande aux répondants d'enregistrer une copie de leur document PDF (2003 ou version plus récente) sur quatre clés USB et d'envoyer celles-ci par courrier à l'adresse mentionnée à la section 2.8.

Les réponses à cette LI peuvent être rédigées dans l'une ou l'autre des langues officielles du Canada, soit en anglais ou en français.

2.7 Demandes d'information

Toute demande d'information ou toute autre communication liée à cette LI et aux activités d'engagement connexes de l'industrie devra être adressée exclusivement à l'autorité contractante de TPSGC. Comme il ne s'agit pas d'une demande de soumissions, le Canada ne répondra pas nécessairement par écrit et ne distribuera pas forcément les réponses à l'ensemble des répondants; toutefois, les répondants qui ont des questions concernant la présente LI peuvent les transmettre à :

Autorité contractante : Patti Wight

Travaux publics et Services gouvernementaux Canada

Place du Portage, Phase III, 18c2
11, rue Laurier
Gatineau (Québec)
K1A 0S5

Adresse de courriel : patti.wight@tpsgc-pwgsc.gc.ca

Téléphone : 819-420-1757

Les communications par courriel doivent être privilégiées.

2.8 Présentation des réponses

Date et lieu de présentation des réponses : Les fournisseurs intéressés devraient présenter leur réponse à l'autorité contractante dont le nom est indiqué ci-dessus, au plus tard à l'heure et à la date indiquées à la page 1 de la présente demande.

La date de clôture de la LI publiée dans les présentes n'est pas la date limite pour faire des commentaires. Les commentaires seront acceptés jusquà ce que l'invitation à soumissionner soit publiée (le cas échéant).

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

Renvoi des réponses : Les réponses à la présente LI ne seront pas renvoyées.

2.9 Surveillant de l'équité

Si un processus d'approvisionnement pour une solution de Sensibilisation à la cybersécurité est lancé dans le futur, le Canada fera appel aux services d'une organisation à titre de tiers indépendant en vue d'agir comme surveillant de l'équité.

Le Canada a retenu les services d'une organisation à titre de tiers indépendant en vue d'agir comme surveillant de l'équité dans le cadre du processus d'approvisionnement. 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 :

i. 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);

ii. Faire part au Canada de ses commentaires sur des questions relatives à l'équité;

iii. Attester l'équité du processus d'approvisionnement.

Afin de s'acquitter de ses obligations, le surveillant de l'équité se verra autoriser l'accès aux réponses de l'industrie et à la correspondance connexe reçue par le Canada en vertu de la présente LI (de même qu'en vertu de toute LI subséquente et de toute DP connexe) et pourra, à titre d'observateur, assister aux activités de suivi en matière d'engagement et de passation de contrats.

PARTIE II : SENSIBILISATION À LA CYBERSÉCURITÉ; CONTEXTE; OBJECTIFS; EXIGENCES EN MATIÈRE DE SÉCURITÉ, EXCEPTION AU TITRE DE LA SÉCURITÉ NATIONALE, POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (RIT), DE LANGUES OFFICIELLES ET; STRATÉGIE D'ENGAGEMENT

3. CONTEXTE DE LA SOLUTION DE SENSIBILISATION À LA CYBERSÉCURITÉ

3.1 Le MDN et les FAC ont besoin d'un système qui assurera une connaissance technique globale de l'emplacement, de l'état et de la configuration de l'infrastructure de technologie de l'information (ITI) des FAC et de la technologie des champs de bataille en réseau afin de réduire la vulnérabilité, d'accroître l'imputabilité et d'assurer la réussite des missions.

3.2 Le projet du Sensibilisation à la cybersécurité en est actuellement à la première phase d'AO en vue de réaliser l'AR requise et d'obtenir l'approbation du projet.

4. OBJET DE LA LETTRE D'INTÉRÊT

4.1 La présente LI est diffusée dans l'objectif suivant :

i. Consulter l'industrie pour déterminer les solutions commerciales actuellement disponibles.

ii. Obtenir de l'information de l'industrie sur le prix et la disponibilité de solutions commerciales.

iii. Fournir de l'information pour aider le MDN et les FAC à élaborer leurs besoins et contribuer au processus d'approbation et de planification interne qui pourrait éventuellement mener à l'établissement d'une demande de soumissions.

4.2 La présente LI ne signifie pas que le Canada a pris sa décision définitive quant aux possibilités d'approvisionnement. Le Canada peut décider de ne choisir aucune des solutions ni aucun équipement indiqués dans les réponses. Le Canada ne sera en aucun cas tenu responsable envers un répondant qui fournira une réponse dans le cadre de la présente LI.

5. EXIGENCES EN MATIÈRE DE SÉCURITÉ

5.1 La LI ne comporte aucune exigence relative à la sécurité.

5.2 Les fournisseurs pourraient être tenus de disposer de la cote de sécurité SECRET, et possiblement TRÈS SECRET, émise par leur programme national de sécurité industrielle respectif pour toute mesure d'approvisionnement à venir prise à l'appui de la solution Sensibilisation à la cybersécurité.

6. EXCEPTION AU TITRE DE LA SÉCURITÉ NATIONALE

6.1 Afin de protéger la souveraineté de ses données et l'intérêt national, le Canada invoque son droit prévu par les accords commerciaux nationaux et internationaux d'utiliser une exception au titre de la sécurité nationale (ESN) dans le cadre de la présente initiative d'approvisionnement.

L'ESN permet au Canada de soustraire l'approvisionnement à certaines ou à l'ensemble des modalités d'un accord commercial pertinent lorsqu'il le juge nécessaire afin de protéger ses intérêts en matière de sécurité nationale ou des intérêts connexes précisés dans le libellé des ESN.

7. POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (RIT)

7.1 Ce besoin n'est pas visé par les accords commerciaux internationaux et s'inscrit dans le cadre de la Stratégie d'approvisionnement en matière de défense annoncée le 5 février, 2014. Par conséquent, la Politique des retombées industrielles et technologiques (RIT) avec la proposition de valeur pourrait être appliquée. La Politique de RIT est administrée par Innovation, Sciences et Développement économique Canada (ISDE). Pour de plus amples renseignements sur la Politique de RIT du Canada, veuillez visiter le site web du ISDE à www.canada.ca/rit.

8. LANGUES OFFICIELLES

8.1 Tout contrat éventuel pour une solution de passeport électronique exigera de l'entrepreneur qu'il fournisse toute la documentation, de même que le soutien technique et le soutien au client dans les deux langues officielles.

9. STRATÉGIE D'ENGAGEMENT

9.1 Engagement de l'industrie

Le processus de mobilisation de l'industrie commence par l'envoi de la présente LI et prend fin au moment où une demande de propositions officielle ou un autre processus concurrentiel est transmis aux fournisseurs. Puisque le MDN et les FAC en sont à la première phase d'AO de l'approvisionnement, l'approche de mobilisation de l'industrie au-delà de la phase 1 est en cours d'élaboration.

Phase 1 – Rétroaction initiale de l'industrie

La présente LI est affichée sur achatsetventes.gc.ca pour permettre à l'industrie de faire part à Travaux publics et Services gouvernementaux Canada et au MDN de renseignements sur le marché actuel, la technologie disponible et les capacités des fournisseurs.

PARTIE III: QUESTIONS À L'INTENTION DE L'INDUSTRIE

10. QUESTIONS À L'INTENTION DE L'INDUSTRIE

10.1 Pour chacune des options 2 à 4 décrites à l'annexe D, les soumissionnaires sont invités à formuler des commentaires, des conseils ou des recommandations en ce qui concerne chacun des critères mentionnés dans le tableau D1.

10.2 Exigences opérationnelles et techniques

10.2.1 Pour chacune des exigences opérationnelles et techniques décrites à l'annexe C, quelle est la façon la plus appropriée de mesurer le rendement d'une solution particulière dans son ensemble et de chacun des éléments qui la composent? Le rendement peut-il être défini de manière mesurable, comme le nombre d'événements par minute ou la durée totale de balayage d'un appareil, ou de toute autre manière facilement reconnaissable? Dans l'affirmative, veuillez préciser.

10.2.2 En quoi la complexité d'une solution change-t-elle en fonction :

a. du nombre d'utilisateurs sur le réseau, tant ceux qui en font un usage général que ceux ayant des privilèges élevés?
b. du nombre d'applications logicielles sur le réseau – applications bureautiques et spécialisées et applications de gestion de réseau?
c. du nombre de serveurs sur le réseau?
d. du nombre de points d'accès aux postes de travail sur le réseau?
e. du nombre de routeurs ou de commutateurs?
f. du nombre et du type de points de présence?
g. du nombre d'adresses IP comprises dans tous les domaines?
h. de la largeur de bande de liaison et du temps d'attente?
i. de la nature délicate des données du point de vue de la sécurité?
j. du contexte de menace?
k. du rythme des opérations?
l. du niveau d'administration de la technologie de l'information (TI) du modèle d'évolution des capacités?
m. du rythme d'évolution des biens de TI au sein de l'infrastructure de TI dans son ensemble?
n. du niveau de confiance du personnel qui utilise le système?
o. du nombre de passerelles d'accès à distance aux réseaux externes et de la nature de ces dernières?
p. de la répartition géographique des composants du réseau?
q. du taux d'incidents de sécurité?

10.2.3 En quoi la complexité d'une solution change-t-elle en fonction du réseau, selon que ce dernier utilise des postes clients lourds traditionnels ou une infrastructure de bureau virtuel hébergé centralisée? Peut-on effectuer une analyse de rentabilisation afin de remplacer l'infrastructure existante par un environnement de bureau virtuel hébergé ou un environnement axé sur l'infonuagique en vue de réduire la complexité et le coût d'une solution?

10.2.4 Quels sont les avantages et les inconvénients des solutions axées sur les agents d'extrémité par rapport aux outils centralisés de découverte de réseau? Est-il nécessaire d'utiliser ces deux types de solutions sur le réseau?

10.2.5 Indiquez les améliorations possibles en matière de technologie dont le ministère de la Défense nationale et les Forces armées canadiennes devront éventuellement tenir compte dans leurs exigences, au cours des 10 prochaines années?

10.3 Facteurs de coût

10.3.1 Quels sont les principaux facteurs de coût associés à cette solution particulière dans son ensemble et à chacun des éléments qui la composent?

10.3.2 Les coûts sont-ils liés directement ou indirectement, de façon mesurable, à ce qui suit :

a. au nombre d'utilisateurs sur le réseau, tant ceux qui en font un usage général que ceux ayant des privilèges élevés?
b. au nombre d'applications logicielles sur le réseau – applications bureautiques et spécialisées et applications de gestion de réseau?
c. au nombre de serveurs sur le réseau?
d. au nombre de points d'accès aux postes de travail sur le réseau?
e. au nombre de routeurs ou de commutateurs?
f. au nombre et au type de points de présence?
g. au nombre d'adresses IP comprises dans tous les domaines?
h. à la largeur de bande de liaison et au temps d'attente?
i. à la nature délicate des données du point de vue de la sécurité?
j. au contexte de menace?
k. au rythme des opérations?
l. au niveau d'administration de la TI du modèle d'évolution des capacités?
m. au rythme d'évolution des biens de TI au sein de l'infrastructure de TI dans son ensemble?
n. au niveau de confiance du personnel qui utilise le système?
o. au nombre de passerelles d'accès à distance aux réseaux externes et à la nature de ces dernières?
p. à la répartition géographique des composants du réseau?
q. au taux d'incidents de sécurité?
r. à tout autre descripteur quantitatif du système? Veuillez préciser.

10.3.3 Donnez un exemple d'un modèle de coûts recommandé, qui utilise un ou plusieurs des descripteurs quantitatifs indiqués au paragraphe précédent.

10.3.4 Si possible, fournissez une estimation indicative des coûts (séparés par catégorie, à savoir la gestion de projet, les services d'ingénierie [en précisant la durée prévue] et les coûts associés au matériel et aux logiciels) pour les tâches suivantes :

a. élaboration des spécifications détaillées du système;
b. élaboration de la conception détaillée du système;
c. méthode d'établissement des coûts et processus de définition des tâches de surveillance des biens de TI;
d. création et déploiement d'un environnement d'essai et de développement;
e. élaboration et déploiement d'un prototype de système;
f. évaluation de sécurité et autorisation;
g. évaluation des besoins en matière de formation;
h. matériel ou logiciels supplémentaires;
i. autres questions liées à la configuration, au paramétrage, à l'installation ou au déploiement;
j. services d'ingénierie divers;
k. coûts d'exploitation (incluant le nombre prévu d'employés à affecter aux services de soutien ou d'analyse des données en vue de la livraison de la solution);
l. coûts liés au soutien en service et à l'entretien.

10.4 Risque

10.4.1 Pour chacune des exigences opérationnelles et techniques décrites à l'annexe C, formulez des commentaires, des conseils ou des recommandations en ce qui concerne :

a. faisabilité technique, y compris la sélection et l'instruction du personnel;
b. gestion de projet;
c. sécurité;
d. approvisionnement, y compris la méthode de passation des marchés privilégiée;
e. soutenabilité;
f. coût;
g. calendrier.

10.4.2 Quel modèle de fixation des prix serait le plus avantageux pour le Canada? Est-il recommandé d'examiner les prix à intervalles réguliers pendant la durée des contrats?

10.4.3 Quelle méthode de passation des marchés serait à privilégier au cours de la durée de vie de la capacité, c.-à-d. un prix de lot ferme ou une certaine forme de limitation des dépenses? Quels renseignements seraient nécessaires afin de fournir une estimation des coûts améliorée pour faciliter l'établissement d'un prix de lot ferme?

10.4.4 Quelle devrait être la durée des contrats (en incluant les années d'option)?

10.4.5 Formulez des recommandations concernant l'approche adoptée pour l'évaluation technique des propositions des fournisseurs.

10.4.6 Formulez des recommandations concernant les exigences imposées en vue d'optimiser la capacité concurrentielle et de réduire les coûts. Quels facteurs contribuent à hausser les tarifs et les autres coûts d'approvisionnement?

ANNEXE A : DESCRIPTION GÉNÉRALISÉE D'UN MODÈLE D'INFRASTRUCTURE RÉSEAU

1 PRÉSENTATION

1.1.1 La présente annexe fournit une description générale non classifiée de haut niveau d'un modèle d'infrastructure réseau en vue de permettre aux fournisseurs éventuels d'estimer et d'évaluer la portée et le degré de complexité des exigences du projet. Des renseignements plus détaillés seront communiqués aux fournisseurs ayant les autorisations de sécurité appropriées à une étape ultérieure du processus de consultation de l'industrie.

1.1.2 Les fournisseurs sont invités à examiner l'information fournie pour être en mesure d'expliquer les facteurs de coûts de la solution et la façon dont les descripteurs quantitatifs décrits ci-dessous peuvent être utilisés pour indiquer les coûts de la solution pour chaque spécification ou exigence de performance définie à l'annexe C.

2 DESCRIPTION GÉNÉRALE

2.1 Introduction

2.1.1 Le modèle d'infrastructure réseau est un réseau d'entreprise Windows Server type basé sur Active Directory, qui fonctionne sur un réseau étendu utilisant le protocole TCP/IP (Protocole de contrôle de transmission/Protocole Internet). Le contrôle à distance, la gestion des correctifs, le déploiement des systèmes d'exploitation et de la plupart des logiciels, la protection du réseau et d'autres services sont offerts au moyen du System Center Configuration Manager de Microsoft.

2.2 Principaux services

2.2.1 En plus des applications et des services spécialisés offerts, le réseau assure les services de base suivants :

a. service de messagerie électronique à l'aide de MS Exchange et de MS Outlook;

b. hébergement Web;

c. partage de fichiers et d'impression;

d. qualité du service;

e. clavardage, vidéo et voix sur IP.

2.3 Sécurité du personnel

2.3.1 **Utilisateurs possédant un compte pour usage général.** Tous les membres du personnel qui possèdent un compte pour usage général doivent avoir, à tout le moins :

2.3.1.1 une cote de fiabilité approfondie pour les réseaux non classifiés;

2.3.1.2 une autorisation de niveau 2 – SECRET pour les réseaux classifiés de niveau 2.

2.3.2 **Utilisateurs possédant des privilèges élevés.** Tous les membres du personnel qui possèdent un compte avec privilèges élevés (administration) doivent avoir, à tout le moins, une autorisation de niveau 3 – TRÈS SECRET.

3 POINTS DE PRÉSENCE

3.1 Généralités

3.1.1 À chaque emplacement comprenant des biens du modèle d'infrastructure réseau, un point de présence (POP) est établi et est utilisé par les routeurs ou les commutateurs traditionnels pour mettre en place le réseau local (RL). La connexion à ces POP est généralement établie comme suit :

3.1.1.1 si l'emplacement est situé au Canada et que le service y est assuré par une entreprise de télécommunications commerciale, Services partagés Canada (SPC), par l'entremise du fournisseur du système de télécommunications national, établit le POP à un point de démarcation approprié au sein des installations du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC);

3.1.1.2 si l'emplacement *n'est pas* situé au Canada ou que le service *n'y est pas* assuré par une entreprise de télécommunications commerciale, le MDN et les FAC, par l'entremise du fournisseur des systèmes de télécommunications militaires, d'un fournisseur de services de télécommunications commercial approprié ou de toute autre ressource ministérielle assurant la connexion réseau du gouvernement canadien, établissent le POP à un point de démarcation approprié au sein des installations du MDN et des FAC au moyen d'un serveur d'accès à distance (RAS);

3.1.1.3 l'accès à distance dans les emplacements déployés (au Canada ou à l'étranger) est établi par les utilisateurs aux points d'accès, qui accèdent aux RAS à partir de la connexion Internet locale, d'un système de télécommunications par satellite (SatCom) en série, d'un système de télécommunications militaires protégées par satellite (TMPS) ou du Système mondial de communications par satellite à large bande (WGS).

3.2 Réseau local logique ou physique

3.2.1 À l'emplacement de certains POP, les composants matériels d'un RL logique peuvent être répartis dans différents bâtiments ou même dans d'autres POP. Il est donc impossible de présumer que la bande passante disponible sur un RL logique est uniforme à tous les points d'accès de ce RL.

4 DESCRIPTEURS QUANTITATIFS DE L'INFRASTRUCTURE DE TECHNOLOGIE DE L'INFORMATION

4.1 Biens de technologie de l'information

4.1.1 Le tableau E 1 fournit un résumé des principaux descripteurs utilisés pour définir la taille, la portée et la nature du modèle d'infrastructure réseau du point de vue des biens de technologie de l'information (TI).

Tableau E 1 – Descripteurs quantitatifs

Descripteur	Quantité	Nombre typique d'utilisateurs à l'emplacement	Nombre typique de points d'accès à l'emplacement
Utilisateurs	15 000		
Utilisateurs possédant un compte pour usage général	14 800		
Utilisateurs possédant des privilèges élevés (administration)	200		
Applications logicielles – applications de bureau et de gestion de réseau et applications spécialisées	150		
Serveurs :	1 000		
Contrôleurs de domaine de Microsoft (MS Windows Server et Active Directory)	70		
Serveurs MS Exchange	30		
Serveur VMware	2		
Serveurs d'applications spécialisés	900		

Descripteur	Quantité	Nombre typique d'utilisateurs à l'emplacement	Nombre typique de points d'accès à l'emplacement
Points d'accès aux postes de travail :	10 000		
Client lourd (Windows 7 – ordinateur de bureau/ordinateur portatif)	8 000		
Appareils bureautiques virtuels hébergés aux points d'accès (VMware)	2 000		
Routeurs ou commutateurs (plusieurs types et modèles de fournisseurs)	800		
Nombre total d'adresses IP dans tous les domaines	20 000		
POP :	125		
Centre urbain au Canada établi par SPC	50	250	175
Accès à distance – Internet	25	15	10
Accès à distance – emplacement déployé – SatCom en série	10	75	50
Accès à distance – emplacement déployé – WGS	20	30	20
Accès à distance – emplacement déployé – TMPS	20	30	20

4.2 Caractéristiques des centres de données

4.2.1 Consulter le Tableau E 2 pour obtenir une description des caractéristiques des centres de données pour le modèle d'infrastructure réseau.

Tableau E 2 – Caractéristiques des centres de données

Centre de données	Capacité	Remarques
Centre national nº 1	60 pétaoctets	Gestion des données de l'utilisateur, installation et entretien des logiciels, gestion des paramètres de l'utilisateur, installation de systèmes d'exploitation à distance, fourniture d'une capacité de traitement et de stockage, infrastructure bureautique virtuelle, service de récupération opérationnelle et archivage de données
Centre national nº 2	60 pétaoctets	
Emplacement typique déployé (de 10 à 15 simultanément)	100 téraoctets	

4.3 Caractéristiques des liaisons de données

4.3.1 Consulter le Tableau E 3 pour obtenir une description des différentes caractéristiques des liaisons de données entre les POP.

Tableau E 3 – Caractéristiques des liaisons de données

Type de liaison de données	Connectivité	Latence	Largeur de bande	Fiabilité
Centre urbain au Canada établi par SPC	> 99 %	< 250 ms	20 Mbps	> 99 %
Accès à distance – Internet	> 85 %	< 250 ms	De 128 Kbps à 10 Mbps	> 75 %
Accès à distance – emplacement déployé – SatCom en série	De 25 à 84 %	De 250 à 1 000 ms	De 128 à 256 Kbps	< 75 %
Accès à distance – emplacement déployé – WGS	> 85 %	De 250 à 1 000 ms	125 Mbps	> 75 %
Accès à distance – emplacement déployé – TMPS	De 25 à 84 %	De 250 à 1 000 ms	De 128 Kbps à 2 Mbps	< 75 %

5 CENTRE D'EXPLOITATION DE RÉSEAU

5.1 Introduction

5.1.1 Le centre d'exploitation de réseau exerce, en tout temps, les activités suivantes en vue d'assurer la défense globale des réseaux contre les cyberexploits : opérations de défense des systèmes informatiques, exploitation des réseaux, gestion des incidents et interventions connexes, opérations de sécurité des réseaux, connaissance de la situation de l'infrastructure de TI et services auxiliaires.

5.2 Outils

5.2.1 Le contrôle des réseaux assuré par le centre d'exploitation de réseau est effectué principalement à l'aide du System Center Operations Manager de Microsoft, des outils de gestion des incidents et de l'information de sécurité connexes et d'autres produits disponibles dans le commerce.

5.2.2 À l'aide de ces outils, le centre d'exploitation de réseau effectue les tâches suivantes :

a. **Agrégation de données :** La solution de gestion des journaux regroupe les données provenant de nombreuses sources, y compris des réseaux, des dispositifs de sécurité, des serveurs, des bases de données et des applications, ce qui permet de consolider les données contrôlées pour éviter de manquer des événements cruciaux;

b. **Corrélation :** Permet de rechercher des attributs communs et de regrouper des événements de façon à créer des ensembles significatifs. Les outils de gestion des incidents et de l'information de sécurité offrent la capacité d'appliquer diverses techniques de corrélation en vue d'intégrer différentes sources et ainsi de transformer des données en renseignements utiles;

c. **Alerte :** L'analyse automatisée des événements mis en corrélation et la production d'alertes permettent d'aviser les destinataires des problèmes à régler dans l'immédiat. Les alertes peuvent être transmises sur un babillard ou envoyées au moyen d'un mécanisme tiers, tel que la messagerie électronique;

d. **Babillards :** Les outils peuvent prendre les données d'un événement et les transformer en diagrammes informatifs pour voir des tendances ou cerner des activités qui ne forment pas des tendances standard;

e. **Conformité :** Les applications peuvent être utilisées pour automatiser la collecte de données sur la conformité et ainsi produire des rapports adaptés en fonction des processus de sécurité, de gouvernance et de vérification existants;

f. **Conservation :** Le stockage à long terme des données historiques est utilisé pour faciliter la corrélation des données au fil du temps et fournir la capacité de conservation nécessaire pour répondre aux exigences de conformité. La conservation des données de journaux à long terme est essentielle dans le cadre des enquêtes judiciaires, puisqu'il est peu probable qu'une faille dans le réseau soit découverte dès que celle-ci apparaît;

g. **Gestion des incidents et mesures correctives :** Offre la capacité d'intervenir lors d'un incident, de faire enquête, de déterminer la source et les causes profondes de l'incident et de mettre en œuvre des mesures correctives pour corriger ou contrôler la situation;

h. **Analyse judiciaire :** Offre la capacité d'effectuer des recherches dans les journaux conservés sur divers nœuds pour différentes périodes, en fonction de critères particuliers. Cela permet d'éviter d'avoir à regrouper soi-même les données de journaux ou d'avoir à chercher dans des milliers de journaux.

ANNEXE B : ENVIRONNEMENTS DE MISSION ET SCÉNARIOS OPÉRATIONNELS

1 PRÉSENTATION

1.1 Renseignements généraux

1.1.1 La présente annexe fournit une description générale des scénarios opérationnels et des environnements de mission de base dans lesquels les cyberopérations défensives du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) seront menées.

1.2 Définitions

1.2.1 Dans le contexte de la doctrine canadienne, voici les définitions fournies dans la Note de doctrine interarmées des FAC sur les cyberopérations (V2).

a. **Cybersécurité** – La cybersécurité établit les fondements d'une défense efficace et la principale responsabilité est de préparer le terrain pour offrir des mesures d'assurance de la mission à l'égard d'une panoplie de menaces. La sécurité englobe la sécurité physique, la sécurité opérationnelle et la cybersécurité; la cybersécurité s'entend de l'offre continue de services et de soutien pour l'usage courant du cyberespace dans le cadre des opérations quotidiennes, notamment l'envoi de courriels et l'utilisation d'applications ou d'Internet.

b. **Cyberdéfense** – La cyberdéfense touche le mandat du MDN et des FAC en matière de défense. Sur le plan stratégique, la cyberdéfense désigne les opérations militaires menées dans le cyberdomaine pour soutenir l'atteinte d'objectifs militaires. Pour comprendre la différence concrète entre la cybersécurité et la cyberdéfense, il faut savoir que la cyberdéfense suppose une transition de l'assurance du réseau (sécurité) vers l'assurance de la mission et qu'elle est pleinement intégrée à la planification opérationnelle des différentes fonctions interarmées. La cyberdéfense est axée sur la détection, l'orientation et l'engagement d'adversaires pour assurer la réussite de la mission du commandant et pour déjouer ces adversaires. Ce passage de la sécurité à la défense nécessite de mettre l'accent sur le renseignement, la surveillance et la reconnaissance, ainsi que l'intégration des activités de l'état-major de façon à inclure le renseignement, les opérations, les communications et la planification.

c. **Opérations réseau** – Les opérations réseau sont axées sur la sécurité et la protection des systèmes de TI conformément aux pratiques exemplaires de l'industrie. Il s'agit d'activités quotidiennes exécutées pour construire, exploiter, maintenir et protéger le cyberdomaine. Ces activités ont également pour but de fournir et d'exploiter un cyberdomaine sécuritaire pour le MDN et les FAC à l'appui des opérations et de l'utilisation régulière du cyberespace.

1.3 Ensembles d'outils

1.3.1 Dans ces environnements de mission et ces scénarios opérationnels, le personnel responsable des opérations réseau aura accès aux deux ensembles d'outils suivants.

a. Ensemble d'outils de sensibilisation à la cybersécurité :

1) contrôles de sécurité critiques;
2) service de gestion de la configuration;
3) service de gestion du changement;
4) service de gestion des vulnérabilités;
5) gestion intégrée de la sécurité et processus d'évaluation et d'autorisation de sécurité.

b. Ensemble d'outils d'aide à la décision pour les cyberopérations défensives :

1) détection — capacité de surveillance et de consignation des activités réalisées dans l'infrastructure de technologie de l'information (ITI) pour détecter les activités anormales;
2) analyse — analyse d'activités anormales pour déterminer les tendances et les actions malveillantes ainsi que les activités non autorisées;
3) rapports et aides à la décision — création de rapports automatisés sur les activités anormales à l'intention des décideurs;
4) mise en œuvre d'intervention — capacité de mettre en œuvre des options programmées ou préprogrammées en matière de cyberopérations défensives pour contrer les activités anormales;
5) échange d'information — capacité d'échanger des rapports et de l'information sur les menaces liées aux activités anormales avec d'autres ministères, les pays membres du Groupe des cinq, les pays membres de l'Organisation du Traité de l'Atlantique Nord (OTAN) et l'industrie.

2 ENVIRONNEMENTS DE MISSION

2.1 National

2.1.1 Les opérations nationales (courantes et d'urgence) pourraient comprendre l'aide aux autorités civiles lors d'interventions en cas de catastrophe naturelle, de cyberattaque, d'attaque terroriste, de crise dans des centres urbains, de menace contre l'infrastructure essentielle, de risque pour les systèmes sanitaires et alimentaires ou d'attaque chimique, biologique, radiologique ou nucléaire (CBRN). Il faudra mieux protéger les ressources canadiennes en raison de l'intensification de la concurrence pour les ressources à travers le monde. Les FAC auront donc besoin de la capacité requise pour assurer une meilleure surveillance à l'échelle nationale. En raison du risque d'augmentation des menaces internes, le MDN et les FAC doivent, dans leur ensemble, s'intégrer davantage à la communauté d'intervention nationale — surtout dans les secteurs de la sécurité et du renseignement. Plus particulièrement, l'environnement de sécurité de l'avenir nécessitera un degré d'intégration entre les organismes à l'échelle nationale qui n'existe pas à l'heure actuelle.

2.2 International

2.2.1 En plus d'être prêtes à défendre le Canada, les FAC doivent pouvoir être déployées à l'étranger dans des régions austères, urbaines et littorales aux prises avec un conflit ou une catastrophe. Les opérations internationales pourraient comprendre l'aide humanitaire, l'évacuation des non-combattants, la reconstruction, les missions de stabilisation ou les combats de grande intensité. Les opérations axées sur les renseignements, les cyberattaques ou les attaques CBRN perpétrées par des organisations terroristes et non étatiques et les menaces conventionnelles sont des éléments potentiels de nos opérations expéditionnaires actuelles et futures. Par conséquent, les FAC de l'avenir devront être une force polyvalente, efficace au combat, qui soit capable de mener à bien une vaste gamme de tâches et de fonctionner dans tous les espaces d'engagement (terrestre, maritime, aérien, spatial et cybernétique). Les FAC doivent poursuivre leurs efforts en vue de devenir une force interarmées, interopérable et intégrée et elles doivent avoir la capacité de travailler dans un environnement où se trouvent des acteurs non étatiques et des organisations non gouvernementales.

2.2.2 Compte tenu des possibilités vastes, incertaines et diverses, voici des scénarios opérationnels de haut niveau dans le cadre desquels le personnel, les processus et les outils des FAC pourraient être déployés :

a. échange et coproduction courants et en temps de paix;
b. opération de préparation à l'intervention en cas de menace asymétrique;
c. opération d'aide humanitaire des Nations Unies;
d. opération coalisée de maintien de la paix;
e. opération coalisée d'application des sanctions;
f. opération coalisée de guerre.

ANNEXE C : EXIGENCES OPÉRATIONNELLES PRÉLIMINAIRES

1 FONCTIONNEMENT GÉNÉRAL

1.1 Contexte

1.1.1 Les Forces armées canadiennes (FAC) doivent posséder une cybercapacité défensive solide, pertinente et souple, à l'intérieur de nos réseaux nationaux et de ceux déployés, en vue d'assurer leur liberté d'action aussi bien dans le cyberespace que de part et d'autre de ce dernier. Compte tenu de l'évolution importante de la cybermenace, il est nécessaire d'élaborer des solutions réseau normalisées offrant des mesures de protection et de défense efficaces. La capacité des FAC à ***protéger*** leur cyberespace est un des principaux piliers qui contribuera à la réussite des missions futures.

1.2 Portée

1.2.1 Le projet est actuellement axé sur l'offre de cyberopérations défensives améliorées dans le domaine SECRET et le domaine désigné déployé (Réseau étendu de la Défense). Une analyse supplémentaire sera effectuée lors de l'étape d'analyse des options pour déterminer l'application optimale de l'aide à la décision pour les cyberopérations défensives au sein du MDN et des FAC.

2 OPÉRATION GÉNÉRALE

2.1 Exigences obligatoires de haut niveau

2.1.1 Un projet de sensibilisation à la cybersécurité efficace mise avant tout sur la protection du cyberespace du ministère de la Défense nationale (MDN) et des FAC, grâce à une évaluation constante de cet environnement, dans le but d'obtenir une connaissance fiable et approfondie, en temps réel, de tous les composants connectés au réseau. Une telle évaluation permettra de mettre en lumière les menaces sous-jacentes et les vulnérabilités techniques des biens essentiels, d'évaluer la conformité sur le plan de la sécurité technique, de soutenir l'établissement des mesures correctives prioritaires et de mettre en œuvre des mesures de cybersécurité. Le projet Sensibilisation à la cybersécurité permettra, s'il y a lieu, de tirer profit des pratiques exemplaires du gouvernement et de l'industrie en matière de sécurité en vue de répondre à ces exigences et favorisera l'adoption de normes communes pour faciliter la collaboration interarmées, interorganisations et interalliés.

2.1.2 L'arrêté du projet Sensibilisation à la cybersécurité définit six exigences obligatoires de haut niveau (EOHN), qui sont présentées dans le tableau ci-dessous. Le degré de réussite du projet dépendra, en partie, de la mesure dans laquelle ce dernier permettra d'établir une capacité qui met en œuvre les contrôles de sécurité critiques définis et qui répond à ces EOHN.

Tableau C 1 – Exigences obligatoires de haut niveau

EOHN	Description
Connaissance technique du réseau (infrastructure de technologie de l'information [ITI])	Méthode automatisée permettant de cibler tous les appareils au sein de l'ITI, qui sont connectés au réseau, et de déterminer leur emplacement (logique et physique) et leur configuration. La sensibilisation à la sécurité de l'ITI doit intégrer les contrôles de sécurité critiques essentiels dans le cadre de la sensibilisation à la sécurité de base.
Détection des vulnérabilités dans l'ITI	Méthode automatisée permettant d'analyser les vulnérabilités dans les configurations existantes.

EOHN	Description
Détection des vulnérabilités causées par les changements apportés au réseau	Analyse des répercussions des changements proposés sur l'ITI du MDN et des FAC.
Changements apportés au réseau à distance et à l'accès au réseau	Être en mesure d'apporter des changements à distance, de façon autonome.
Capacité de fonctionnement dans les environnements à faible bande passante	Être en mesure de fonctionner même sans connexion au réseau ou dans les environnements où la bande passante est limitée.
Interopérabilité	Intégrer des mesures de sécurité et des renseignements aux projets, de même qu'en collaboration avec les partenaires et les alliés, afin d'améliorer la cyberdéfense du MDN et des FAC.

2.1.3 Le présent document est un énoncé des besoins opérationnels qui continuera d'évoluer parallèlement aux discussions avec les intervenants, l'industrie et le milieu opérationnel. Le résultat visé est un énoncé définitif des besoins opérationnels pour une capacité que l'industrie peut fournir et que l'exploitant peut accepter qui aura été approuvé. À cette fin, les définitions du Tableau C 2 seront peaufinées jusqu'à ce que les exigences soient établies définitivement. Par conséquent, le Canada peut décider de modifier / ajouter / supprimer les exigences du système, au besoin.

Tableau C 2 — Activité d'établissement des exigences

Activité
Définition et mise en œuvre d'une suite complète comprenant les moyens techniques, les procédures, le concept des opérations et l'instruction, pour sécuriser, surveiller et mettre à jour l'ITI.
Définition et mise en œuvre d'une solution indépendante du réseau qui sera déployée sur le domaine SECRET et le domaine désigné déployé (Réseau étendu de la Défense déployé).
Définition et mise en œuvre d'une capacité souple intégrant l'ITI pour assurer l'automatisation et la tenue à jour de la sécurité.
Définition et mise en œuvre d'un système permettant l'intégration et l'optimisation d'autres programmes et projets cybernétiques des FAC afin de permettre l'échange d'information.
Définition et mise en œuvre d'un système capable de protéger les appareils et l'information contre les menaces et les capacités actuelles. Grâce à des mises à jour, le système doit être tenu à jour et il doit protéger les appareils de l'ITI contre les nouvelles menaces et capacités des adversaires dans un environnement en mutation. Par exemple, à des fins défensives, le système doit être capable de gérer (c.-à-d. de surveiller, de placer dans le bac à sable ou de déconnecter) tous les appareils compromis ou non autorisés de l'ITI.
Définition et mise en œuvre d'un système personnalisé et conçu pour le personnel du MDN et des FAC qui assure la planification, la conception, l'exploitation, la gestion, la sécurité ou la défense d'un réseau et d'une technologie de champs de bataille en réseau. Ce système est actuellement axé sur le sous-ministre adjoint (Gestion de l'information), les centres du réseau de service, la base et les unités responsables du réseau de la formation. Le projet comprendra des solutions adaptables, nouvelles ou existantes, à la sensibilisation sur la sécurité à l'échelon approprié.

Définition et mise en œuvre d'un système d'instruction que le personnel du MDN et des FAC peuvent utiliser pour veiller à ce qu'ils soient capables d'exploiter les capacités du projet Sensibilisation à la cybersécurité.

2.2 Exigences concernant le système

2.2.1 Le Tableau C 3 présente le sommaire des exigences préliminaires concernant le système, lesquelles sont inspirées des EOHN.

2.2.2 Chaque exigence doit être examinée parallèlement à l'Annexe B – Environnements de mission et scénarios opérationnels, ainsi qu'aux interactions connexes de sensibilisation à la cybersécurité. En outre, le système ou le service découlant du projet Sensibilisation à la cybersécurité doit être conçu pour s'adapter à la nature changeante et dynamique du cyberespace. Il est reconnu qu'il est probablement impossible de protéger l'entreprise contre tous les vecteurs de menaces, mais l'objectif vise à concevoir un système résilient qui assurera les fonctions essentielles de commandement et contrôle dans toutes les situations, tout en préservant la liberté d'action opérationnelle.

Tableau C 3 — Sommaire des exigences concernant le système

Nº	Titre	Description
1	Base de données des configurations et inventaire des biens faisant autorité pour le cyberespace du MDN et des FAC	Établir une liste d'inventaire des biens faisant autorité pour tous les biens autorisés dans le cyberespace du MDN et des FAC; fournir une base de données de gestion des configurations faisant autorité pour tous les biens autorisés dans le cyberespace des FAC; définir la règle d'affectation des noms à utiliser pour le suivi des biens (y compris des types de biens, de leur niveau de criticité, des réseaux, des hôtes virtuels et physiques, des applications, des appareils interzones, etc.).
2	Détection des biens dans le cyberespace du MDN et des FAC	Méthode automatisée permettant de détecter tous les biens connectés au réseau (autorisés et non autorisés) et d'en valider la nature.
3	Évaluation de la vulnérabilité des biens dans le cyberespace du MDN et des FAC	Méthode automatisée permettant d'évaluer les répercussions des vulnérabilités connues (p. ex., données tirées des *Common Vulnerabilities and Exposures*) sur les biens du réseau et d'établir les types de biens dans la liste d'inventaire faisant autorité; soutien pour l'établissement des mesures correctives prioritaires, en ciblant les biens essentiels; capacité de consigner les résultats, de déclencher des alertes et de produire des rapports.
4	Évaluation de la conformité des biens à la configuration requise dans le cyberespace du MDN et des FAC	Méthode automatisée permettant d'évaluer la conformité aux configurations de base autorisées pour tous les biens; soutien pour l'établissement des mesures correctives prioritaires, en ciblant les biens essentiels; capacité de consigner les résultats, de déclencher des alertes et de produire des rapports.
5	Intégration des données provenant d'autres processus et groupes de travail fonctionnels en vue de soutenir les évaluations du projet Sensibilisation à la cybersécurité	Méthode automatisée permettant d'intégrer des renseignements qui font autorité, tels que des données sur la menace, l'inventaire des biens, les vulnérabilités, la gestion des configurations, la gestion des événements et des incidents de sécurité ainsi que les évaluations et les autorisations de sécurité; les sources de données faisant autorité seront hébergées sur des réseaux affichant un degré de confidentialité faible, moyen et élevé.
6	Établissement d'une interface utilisateur configurable pour produire des évaluations de sécurité personnalisées, voir les résultats et transmettre des rapports ou des alertes	Méthode automatisée permettant de demander des évaluations personnalisées, de voir les résultats et de transmettre des rapports ou des alertes; l'utilisateur peut configurer les éléments à afficher; les évaluations peuvent être planifiées ou faites sur demande; une indication est fournie quant à l'ordre de priorité des mesures d'atténuation actuelles.
7	Évaluation des risques découlant des changements proposés aux biens existants présents dans le cyberespace du MDN et des FAC	Méthode automatisée permettant d'analyser les répercussions des changements proposés au cyberespace des FAC (configuration, conception, matériel ou logiciels entièrement nouveaux, mis à jour ou éliminés) et de produire des rapports à cet égard.

Nº	Titre	Description
8	Mesures d'adaptation pour les environnements sans connexion, à connexion intermittente ou à faible bande passante	Une capacité d'évaluation locale doit être établie au sein des environnements sans connexion, à connexion intermittente ou à faible bande passante. Une capacité d'évaluation centralisée doit permettre d'obtenir et d'intégrer des renseignements sur les biens à partir des environnements sans connexion, à connexion intermittente ou à faible bande passante, lorsque les conditions de connexion le permettent.
9	Intégration des données des capteurs de la plate-forme	Méthode automatisée permettant d'intégrer les données transmises par les capteurs de la plate-forme (en supposant qu'une interface de programmation d'applications [API] ou un protocole standard est utilisé) au système de Sensibilisation à la cybersécurité.
10	Intégration des données des technologies d'exploitation	Méthode automatisée permettant d'intégrer les données transmises par les capteurs des technologies d'exploitation (en supposant qu'une API ou un protocole standard est utilisé) au système de Sensibilisation à la cybersécurité.
11	Intégration de mesures d'attribution des tâches et de flux de travaux automatisés pour faciliter les interventions	Automatiser l'attribution des tâches et le flux des travaux en vue de répondre aux éléments déclencheurs dans le système de Sensibilisation à la cybersécurité; intégrer des flux de travaux et définir les processus et les liens existants entre les différentes organisations fonctionnelles; fournir une capacité de suivi et de surveillance des progrès; définir les biens essentiels en vue de faciliter l'établissement des tâches prioritaires.
12	Étiquetage de données	Automatiser l'étiquetage des données du MDN et des FAC et exiger le recours à ce dernier dans les types de dossiers précisés en vue de soutenir l'inventaire des fonds de données, de même que les vérifications de la conformité aux politiques de sécurité.
13	Intégration d'un processus de gestion des risques automatisé	Déterminer, définir, intégrer et automatiser les processus requis pour assurer la gestion des risques (y compris la catégorisation de renseignements, la sélection des contrôles de sécurité, l'évaluation des mesures de protection, la vérification de la conformité des configurations et le calcul du risque).
14	Normes relatives au protocole de communication et au format de données	Les formats de données et les protocoles de communication doivent être conformes aux normes actuelles de l'industrie ou prises en charge par des interfaces de programmation d'application ouvertes.
15	Mise en application de la gestion des privilèges administratifs	Assurer de très près le suivi et la surveillance des comptes d'administration et évaluer périodiquement cette capacité afin d'assurer la conformité. Utiliser une authentification à deux facteurs, lorsqu'il y a lieu, et mettre en œuvre des postes de travail spécialisés pour les fonctions administratives seulement.
16	Système de gestion des correctifs	Automatiser un processus de gestion des correctifs efficace et efficient en vue de déterminer, d'acheter, d'installer et de vérifier les correctifs requis pour tous les produits et les systèmes (commerciaux ou gouvernementaux).

2.3 Classification de sécurité

2.3.1 Le projet Sensibilisation à la cybersécurité doit être mis en œuvre conformément aux exigences du processus du Guide d'évaluation de la sécurité et d'autorisation. Un processus d'évaluation et d'autorisation de sécurité complet sera effectué, ce qui donnera lieu à l'établissement d'une orientation appropriée sur la mise en œuvre du matériel, du logiciel, du personnel et des procédures nécessaires pour satisfaire aux exigences relatives à la capacité de sécurité.

2.3.2 Il est possible que les fournisseurs et leurs sous-traitants doivent accéder à des systèmes et à des données de nature délicate, ce qui peut nécessiter la participation de personnel du niveau approprié et l'obtention des attestations de sécurité d'installation.

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

2.3.4 Compte tenu de la menace associée au cyberdomaine, le matériel et les services visés par le présent projet doivent être fournis en tout temps et de façon continue, assurée et fiable.

2.4 Surviabilité

2.4.1 Le projet Sensibilisation à la cybersécurité doit offrir des fonctions permettant de réduire au minimum la perturbation des opérations causée par des défaillances de composants, conformément aux exigences du processus d'évaluation et d'autorisation de sécurité.

2.5 Maintenance et soutien

2.5.1 Le projet Sensibilisation à la cybersécurité doit être déployé et pris en charge de façon intégrée avec les processus de gestion de la configuration et des changements de l'ITI, autant au MDN qu'à Services partagés Canada.

2.5.2 Le MDN et les FAC devraient posséder des droits de création, de maintenance et de modification de logiciels personnalisés permettant l'interfaçage de sources d'information dans la fonction de sensibilisation à la cybersécurité.

2.5.3 Le projet Sensibilisation à la cybersécurité devrait pouvoir être mis à niveau de façon intégrée, sans tâches de génie logiciel complexes.

2.5.4 Le personnel du projet Sensibilisation à la cybersécurité ne doit avoir besoin que d'une instruction supplémentaire minimale pour effectuer ses tâches.

2.5.5 Le projet Sensibilisation à la cybersécurité doit permettre de quadrupler le nombre de points d'accès, sans aucune mise à niveau du système principal, de l'infrastructure, des composants, du matériel ou des logiciels existants.

2.6 Disponibilité opérationnelle

2.6.1 Les composants essentiels du projet Sensibilisation à la cybersécurité doivent être disponibles xx % du temps, à l'exception des postes de travail (dans l'hypothèse où les utilisateurs peuvent travailler sur plus d'un poste).

2.6.2 Les composants essentiels du projet Sensibilisation à la cybersécurité devraient être disponibles xx % du temps, à l'exception des postes de travail (dans l'hypothèse où les utilisateurs peuvent travailler sur plus d'un poste).

2.7 Fiabilité

2.7.1 La moyenne des temps de bon fonctionnement du projet Sensibilisation à la cybersécurité doit être de 30 jours.

2.7.2 Le temps nécessaire pour réparer le système découlant du projet Sensibilisation à la cybersécurité et le rendre fonctionnel doit être conforme à l'énoncé de la nature délicate et aux exigences du processus d'évaluation et d'autorisation de sécurité.

2.8 Durabilité de l'environnement

2.8.1 Le projet Sensibilisation à la cybersécurité doit respecter les normes du MDN en matière de gérance de l'environnement.

2.9 Santé et sécurité

2.9.1 Le projet Sensibilisation à la cybersécurité ne doit 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.

2.9.2 Le système découlant du projet Sensibilisation à la cybersécurité doit être conforme à tous les codes du MDN et des FAC applicables en matière de santé et de sécurité.

2.10 Exigences relatives à la livraison

2.10.1 Le projet Sensibilisation à la cybersécurité doit inclure un mécanisme de mise à jour et de mise en œuvre de correctifs sécurisé, accessible partout dans le monde à partir des emplacements et des biens approuvés.

2.10.2 Le projet Sensibilisation à la cybersécurité doit servir à tous les utilisateurs (autorités opérationnelles, opérateurs techniques de technologie de l'information [TI] et personnel de soutien) travaillant ensemble dans les lieux de services de TI de la région de la capitale nationale.

2.10.3 Le projet Sensibilisation à la cybersécurité doit servir à tous les utilisateurs (autorités opérationnelles, opérateurs techniques de TI et personnel de soutien) travaillant ensemble :

a. au Canada à l'extérieur des lieux de services de TI de la RCN;

b. à l'étranger à l'extérieur des lieux de services de TI de la RCN dans des lieux de services de TI désavantagés par une bande passante limitée.

2.11 Exigences sur le plan du personnel et de la formation

2.11.1 Le projet Sensibilisation à la cybersécurité doit prévoir une instruction adaptée aux tâches des utilisateurs (autorités opérationnelles, opérateurs techniques de TI et personnel de soutien), conformément à la politique et aux normes pertinentes des FAC et selon les conclusions tirées de l'évaluation des besoins en instruction. Cette exigence comprend les installations, le matériel d'instruction et les formateurs qualifiés contribuant à la capacité opérationnelle initiale, ainsi qu'un système d'instruction continue essentiel à l'établissement de la capacité opérationnelle totale.

2.11.2 Le projet Sensibilisation à la cybersécurité doit comprendre un système d'instruction par simulation qui servira à l'instruction opérationnelle collective dans un contexte opérationnel personnalisable. Les scénarios d'instruction par simulation doivent être créés, mis à jour et exécutés par les opérateurs techniques de TI à l'aide des postes de travail et des systèmes déjà installés dans un environnement d'exercice ou d'instruction.

2.11.3 Le projet Sensibilisation à la cybersécurité doit être conçu en fonction des pratiques exemplaires et des leçons tirées d'opérations et de mesures précédentes.

ANNEXE D : MÉTHODE D'ANALYSE DE RENTABILISATION

1 PRÉSENTATION

1.1 Contexte

1.1.1 Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) ont besoin d'un système qui fournira une connaissance fiable et en temps réel de son infrastructure de technologie de l'information (ITI), de ses applications et de ses données. En automatisant et en intégrant les capacités, les services et les processus suivants, le projet Sensibilisation à la cybersécurité, qui mettra l'accent sur les connaissances, servira de fondement aux initiatives de cyberopérations défensives connexes :

a. contrôles de sécurité critiques;

b. service de gestion de la configuration;

c. service de gestion du changement;

d. service de gestion des vulnérabilités;

e. gestion intégrée de la sécurité et processus d'évaluation et d'autorisation de sécurité.

1.2 Méthode d'analyse de rentabilisation

1.2.1 Le projet Sensibilisation à la cybersécurité en est au début de l'étape de l'analyse des options et l'on s'efforce d'achever l'analyse de rentabilisation requise et d'obtenir l'approbation de projet.

1.2.2 Pour achever l'analyse de rentabilisation, le MDN et les FAC doivent suivre les politiques, les approches, les modèles, les directives et les ressources que le Secrétariat du Conseil du Trésor du Canada a mis en place à l'appui de la saine gestion de projet (consulter le site : http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/itpm-itgp/pm-gp/index-fra.asp).

2 BESOINS OPÉRATIONNELS ET RÉSULTATS SOUHAITÉS

2.1 Présentation

2.1.1 La sécurité du cyberespace[1] doit être assurée, étant donné que le MDN et les FAC dépendent des réseaux informatiques et des réseaux de communication électronique dans tous les aspects de leurs activités de planification et d'exploitation, notamment pour le commandement et le contrôle et l'accès à des ressources logistiques et stratégiques clés. Il est maintenant essentiel d'être en mesure de détecter efficacement les activités malveillantes à l'endroit du cyberdomaine[2] du MDN et des FAC et de prendre les mesures appropriées, en particulier dans la mesure où le cyberdomaine est une cible de plus en plus facile d'accès pour les adversaires potentiels. Afin de défendre efficacement le cyberdomaine, il faut d'abord définir et comprendre l'étendue et la portée de l'ITI[3] du MDN et des FAC.

---

[1] Le cyberespace est le réseau interdépendant de structures des technologies de l'information (TI), ce qui comprend Internet, les réseaux de télécommunication, les systèmes informatiques et les processeurs et contrôleurs intégrés, de même que les logiciels et les données qu'ils contiennent[1].

[2] Le cyberdomaine est un sous-ensemble du cyberespace défini comme la zone du cyberespace où le MDN, les FAC, leurs partenaires, leurs alliés et les auteurs de menace choisissent d'assurer une présence ou d'exercer leurs activités[1].

[3] L'ITI s'entend des ordinateurs, des réseaux et des dispositifs connectés, y compris de tous les logiciels, le matériel et les micrologiciels connexes, qui sont utilisés pour transmettre, traiter ou stocker des données ou pour contrôler des dispositifs mécaniques[2].

2.1.2 Le cyberdomaine de l'adversaire sera de plus en plus ciblé lors des conflits à venir dans l'espoir de réduire les capacités de ce dernier dans tous les domaines. Pour maintenir leur liberté de manœuvre dans un cyberdomaine faisant l'objet d'une attaque, le MDN et les FAC ont besoin d'une ITI sécuritaire et solide. Compte tenu de l'importance des renseignements détenus sur les réseaux du MDN et des FAC, ceux-ci sont la cible des cyberopérations offensives menées par des États-nations, des organismes appuyés par l'État et des acteurs non étatiques et continueront de l'être. Les cyberopérations offensives offrent aux adversaires du Canada une façon de mener des attaques asymétriques, notamment de pénétrer et de perpétrer des attaques dans des infrastructures, des réseaux et des systèmes essentiels ou riches en information.

2.1.3 Le projet Sensibilisation à la cybersécurité a pour but de faire connaître, en temps quasi réel, l'état, la connectivité et l'emplacement de l'ITI utilisée par le MDN et les FAC afin de cibler et de réduire leurs vulnérabilités techniques. En réduisant nos vulnérabilités, nous diminuerons les vecteurs d'attaque dont disposent nos adversaires, ce qui les forcera à utiliser des attaques de plus grande valeur qu'ils pourront mener uniquement à des coûts plus élevés. Le projet Sensibilisation à la cybersécurité permettra de réduire les attaques réussies et de mieux connaître le réseau, ce qui contribuera à la capacité d'aide à la décision pour les cyberopérations défensives et permettra ainsi de cibler et d'atténuer les exploits du « jour zéro[4] » et autres exploits évolués, améliorant par le fait même la sécurité et la protection du réseau dans son ensemble. Ces changements rendront possible l'assurance de la mission, en améliorant la capacité du MDN et des FAC à détecter, à contrer ou à atténuer les opérations offensives et les exploits de leurs adversaires, ce qui permettra au MDN et aux FAC de maintenir leur liberté d'action dans le cyberdomaine.

2.1.4 Tout au long du présent document, il est important de comprendre la différence entre les deux concepts clés suivants, tels qu'ils sont définis dans la Note de doctrine interarmées des FAC sur les cyberopérations, la cybersécurité et la cyberdéfense.

a. **Cybersécurité** – La cybersécurité établit les fondements d'une défense efficace et la principale responsabilité est de préparer le terrain pour offrir des mesures d'assurance de la mission à l'égard d'une panoplie de menaces. La sécurité englobe la sécurité physique, la sécurité opérationnelle et la cybersécurité; la cybersécurité s'entend de ***l'offre continue de services et de soutien pour l'usage courant du cyberespace dans le cadre des opérations quotidiennes***, notamment l'envoi de courriels et l'utilisation d'applications ou d'Internet.

b. **Cyberdéfense** – La cyberdéfense touche le mandat du MDN et des FAC en matière de défense. Sur le plan stratégique, la cyberdéfense désigne les ***opérations militaires menées dans le cyberdomaine pour soutenir l'atteinte d'objectifs militaires***. Pour comprendre la différence concrète entre la cybersécurité et la cyberdéfense, il faut savoir que la cyberdéfense suppose une transition de l'assurance du réseau (sécurité) vers l'assurance de la mission et qu'elle est pleinement intégrée à la planification opérationnelle des différentes fonctions interarmées. La cyberdéfense est axée sur la détection, l'orientation et l'engagement d'adversaires pour assurer la réussite de la mission du commandant et pour déjouer ces adversaires. Ce passage de la sécurité à la défense nécessite de mettre l'accent sur les renseignements, la surveillance et la reconnaissance, ainsi que l'intégration des activités de l'état-major de façon à inclure les renseignements, les opérations, les communications et la planification.

2.2 Besoin opérationnel

2.2.1 Le MDN et les FAC utilisent le cyberdomaine dans toutes leurs activités, notamment pour les annonces publiques, la transmission de courriels classifiés et l'exploitation des réseaux utilisés pour connecter les systèmes de missiles et de radiodétection sur les navires et dans les avions. Malgré cette dépendance au cyberdomaine, les unités, les formations et les bases n'ont pas une très bonne connaissance de la connectivité des réseaux, que

[4] Une vulnérabilité du « jour zéro » est une vulnérabilité non divulguée présente dans une application, qui pourrait être exploitée afin de porter atteinte aux programmes informatiques, aux données, à d'autres ordinateurs ou au réseau. Elle est connue sous le nom de « jour zéro » du fait qu'une fois que la faille est connue, l'auteur de l'application a zéro jour pour planifier et recommander toute mesure d'atténuation pour contrer l'exploitation. Les attaques fondées sur des exploits du jour zéro sont souvent perpétrées le jour même où l'avis de vulnérabilité est rendu public ou même avant; parfois, l'attaque a lieu avant que l'auteur ne connaisse le code corrigé ou ne l'ait élaboré et rendu disponible[3].

l'intégration des technologies de champs de bataille en réseau rend d'autant plus complexes. Elles n'ont pas non plus la capacité, en temps quasi réel, de mettre en corrélation l'information reçue de tous les dispositifs connectés au réseau afin de dresser un portrait global de la situation. Ce manque d'information nuit à la capacité du commandant de prendre des décisions éclairées à l'intérieur du cyberdomaine et porte grandement atteinte à la capacité du MDN et des FAC de sécuriser et de défendre leur ITI. La fréquence d'utilisation de l'ITI par le MDN et les FAC et l'usage diversifié qu'ils en font pour réaliser leurs opérations aggravent cette situation, qui donne lieu à un ensemble de processus et de problèmes d'intégration de plus en plus complexe qui, pour être géré, requiert des efforts soutenus et délibérés.

2.2.2 Le fait que le cyberespace soit la cible des attaques de nos adversaires, qui ont divers objectifs stratégiques et capacités offensives, nuit encore davantage à la capacité du MDN et des FAC à surmonter ces difficultés. Pour fournir au MDN et aux FAC une liberté de manœuvre dans le cyberdomaine, le projet Sensibilisation à la cybersécurité doit permettre de recueillir et d'évaluer des renseignements dynamiques concernant la sécurité, la configuration et l'état du réseau, ce qui améliorera la capacité du MDN et des FAC à défendre leur ITI.

2.2.3 Le MDN et les FAC ont besoin d'une connaissance technique globale de l'emplacement (logique et physique), de l'état et de la configuration de l'ITI du MDN et des FAC. Cette information permettra d'accroître la responsabilité à l'égard de l'équipement du MDN et des FAC et améliorera la sécurité du réseau, en permettant l'accès à de plus amples renseignements, ce qui rendra possibles des interventions adaptées en réponse aux cyberévénements. Grâce aux connaissances acquises au moyen de ce système pleinement automatisé, le MDN et les FAC pourront créer, exploiter et contrôler un réseau normalisé et étendu, mais surveillé de façon centralisée. La confirmation de la conformité aux normes pourra être maintenue, et le processus d'ingénierie utilisé pour apporter des modifications aux réseaux et aux technologies de champs de bataille en réseau[5] pourra être quantifié et vérifié. La connaissance des dispositifs en réseau permettra également de prendre des mesures de sécurité améliorées à l'égard des principaux cyberterrains ciblés ou des zones de cybervulnérabilité connues jugées essentielles aux opérations.

2.3 Facteurs de changement

2.3.1 Les cybercapacités défensives et la sécurité des FAC doivent s'améliorer et évoluer au même rythme que la sécurité et les cybercapacités défensives de ses adversaires. Le MDN et les FAC doivent être prêts à protéger le cyberdomaine pour assurer l'utilisation continue de l'ITI en réseau et continuer de profiter des avantages militaires qui en découlent. Dans le Plan d'action 2010 de la Stratégie de cybersécurité du Canada, le gouvernement du Canada a chargé le MDN de renforcer sa capacité à défendre ses réseaux. Pour ce faire, l'étendue du réseau et l'état de ce dernier doivent être connus des intervenants, qui doivent pouvoir prendre des mesures concrètes aux niveaux stratégique, opérationnel et tactique. La représentation des réseaux doit également inclure les principales technologies de champs de bataille en réseau, qui sont de plus en plus un vecteur d'attaque pour les adversaires. Bien qu'une partie de cette information soit déjà accessible, le projet Sensibilisation à la cybersécurité permettra d'établir un dépôt commun exploitable.

2.3.2 Les capacités de défense et de sécurité actuelles ont été créées et influencées par les leçons retenues à l'époque où le cyberdomaine, la sécurité de la TI et la défense des réseaux en étaient à leurs balbutiements; les processus administratifs étaient effectués sur papier, les fonctions pouvaient être centralisées autour de simples organisations, les menaces se concrétisaient lentement comparativement à aujourd'hui, les systèmes n'étaient pas intégrés, les vulnérabilités étaient peu fréquentes et les risques pouvaient être quantifiés avec précision, étant donné que les systèmes étaient relativement peu complexes. Chacune de ces caractéristiques a subi des changements radicaux au cours des 10 dernières années, qui se sont traduits par une augmentation progressive de leur portée, de leur importance, de leur complexité et du rythme de leur évolution. Afin de composer avec les environnements opérationnels actuels et futurs, le MDN et les FAC doivent laisser tomber le modèle centré sur

[5] Dans le présent document, les technologies de champs de bataille en réseau font référence à l'ensemble des outils qui ne seraient pas normalement considérés comme faisant partie du réseau, mais qui, dans le domaine militaire, permettent une meilleure connectivité réseau ou sont améliorés grâce à l'utilisation d'un réseau. Cela inclut les nœuds non traditionnels, notamment les radios, les missiles et l'intégration radar.

les organisations, où les activités sont réalisées manuellement sur support papier, pour en adopter un où les activités s'appuient sur une capacité d'entreprise, qui permet des interventions décentralisées définies, mais indépendantes, une visibilité à plusieurs niveaux et une coordination verticale et qui intègre l'information d'entreprise provenant des différents réseaux et plates-formes d'armes, de même que de multiples points de vue et visions de la situation opérationnelle, en fonction des besoins.

2.3.3 Les failles dans les logiciels et la configuration inappropriée des composants des systèmes d'information sont des vulnérabilités majeures, qui permettent d'exploiter ces systèmes. Le SANS Institute, une organisation de recherche et de formation en matière de sécurité, qui est respectée et réputée mondialement, a produit un rapport sur les 20 principaux contrôles de sécurité critiques pour les systèmes d'information, en collaboration avec la National Security Agency et d'autres organismes américains nationaux et internationaux.

2.3.4 Les quatre plus importants contrôles sont les suivants :

a. Liste des appareils autorisés et non autorisés;

b. Liste des logiciels autorisés et non autorisés;

c. Configurations sécurisées pour le matériel et les logiciels : appareils mobiles, ordinateurs portatifs, postes de travail et serveurs;

d. Évaluation continue de la vulnérabilité et restauration.

2.3.5 Le projet Sensibilisation à la cybersécurité permettrait de s'assurer que ces contrôles sont mis en place, améliorant ainsi grandement la cybersécurité du MDN et des FAC.

2.4 Résultats opérationnels

2.4.1 Le projet Sensibilisation à la cybersécurité permettra de définir et de diffuser une série de processus opérationnels et de jeux d'outils intégrés, qui seront utilisés pour recueillir de façon dynamique des renseignements sur la conception, la configuration et l'état pour l'ITI du MDN et des FAC, dans le but de réaliser des activités de planification, d'exploitation, de sécurité et de défense essentielles. Ce projet fournira une plate-forme pour l'intégration de nouvelles suites de sécurité ou le remplacement de celles déjà en place et contribuera à l'établissement d'un environnement de sécurité étendu, qui sera axé non seulement sur la cybersécurité, mais également sur la sécurité physique, personnelle et administrative. Combinés, ces éléments amélioreront la capacité du MDN et des FAC à protéger et à défendre avec plus d'assurance leur ITI dans cet environnement exposé aux attaques. Ce projet sera associé à d'autres mesures de sécurité et de défense prises par le MDN, les FAC, le gouvernement du Canada, leurs partenaires et leurs alliés.

2.4.2 Le projet Sensibilisation à la cybersécurité créera une plate-forme d'intégration des données, qui servira de fondement pour la collecte de données automatisée, l'établissement de capacités avancées en matière de défense des réseaux et d'atténuation des menaces, l'obtention d'une connaissance intégrée des opérations essentielles de l'ITI et l'adoption de processus continus de gestion des risques. En vue de mettre en place ces capacités, les responsables du projet chercheront à mettre à jour les outils vieillissants, à intégrer ou à remplacer les outils en service existants et à introduire des technologies futures qui soutiennent les activités de sécurité, incluant notamment : l'analyse et la gestion des vulnérabilités, la gestion des incidents, la vérification et la surveillance des réseaux, la gestion de la configuration, du changement et des mesures d'atténuation, les activités de soutien du renseignement, les évaluations et les autorisations de sécurité, ainsi que les activités de sécurité qui ont un lien avec l'ITI. Le projet Sensibilisation à la cybersécurité remplacera les données de sécurité cloisonnées et les processus manuels utilisés actuellement par des processus administratifs automatisés et corrélés dans les secteurs d'activité ciblés.

2.4.3 **Résultats opérationnels directs.** Le projet Sensibilisation à la cybersécurité permettra au gouvernement du Canada d'obtenir les résultats opérationnels directs suivants.

2.4.3.1 Économies importantes sur le plan de la main-d'œuvre par l'automatisation de la collecte de données, de l'analyse et de la coordination des interventions, ayant pour résultat :

a. la diminution du nombre d'employés qui répondent aux problèmes liés à l'équipement et qui traitent les données;

b. l'élimination du dédoublement des efforts entre le personnel technique chargé de la technologie de l'information (TI) et les responsables des opérations des réseaux;

c. la diminution du temps d'inspection à l'égard des lacunes et des problèmes associés aux biens de TI;

d. la réduction du délai de récupération de l'information relative aux configurations de sécurité et à l'état des biens de TI.

2.4.3.2 Économies relatives aux investissements dans les biens de TI et au soutien en service grâce à :

a. une meilleure compréhension de l'état des biens de TI, qui mènera à la réparation de l'équipement existant ou à l'achat de matériel de remplacement au moment opportun, en fonction des données réelles sur l'état de ces biens;

b. la réduction des coûts directs liés aux voyages ou d'autres coûts de transport associés à la gestion de l'état des biens de TI dans différents emplacements;

c. la réduction du nombre d'employés contractuels temporaires chargés de gérer les configurations et l'état des biens de TI.

2.4.4 **Résultats opérationnels indirects.** En plus des résultats opérationnels directs, le projet Sensibilisation à la cybersécurité permettra d'obtenir les résultats opérationnels indirects suivants :

a. réduction des coûts et du temps d'instruction;

b. amélioration de la sécurité des données et de la protection des biens;

c. amélioration du temps de réponse au moment d'offrir un soutien et de répondre aux demandes concernant l'état des biens de TI;

d. gestion de la configuration détaillée et suivi des biens de TI en temps quasi réel;

e. amélioration de la conformité aux lois et aux politiques concernant la sécurité des systèmes d'information et la protection des données.

2.4.5 **Résultats opérationnels qualitatifs.** Au fur et à mesure que la capacité offerte par le projet Sensibilisation à la cybersécurité évoluera, le MDN et les FAC obtiendront les résultats qualitatifs suivants :

a. disponibilité accrue de l'information sur la gestion en lien avec l'ITI dans son ensemble;

b. intégrité accrue des données en ce qui concerne l'ITI;

c. meilleures connaissances organisationnelles (conservation et récupération) au sujet du rendement du système, de l'état de sécurité, des risques, des menaces et des vulnérabilités ainsi que des coûts;

d. satisfaction accrue des commandants, des gestionnaires et des cadres supérieurs ministériels responsables de l'information classifiée;

e. renforcement de la confiance du public à l'égard de la capacité du MDN et des FAC d'assurer la sécurité de l'information et des biens classifiés;

f. renforcement de la confiance des alliés à l'égard de la capacité du MDN et des FAC d'assurer la sécurité de l'information et les biens classifiés;

g. processus décisionnel plus efficace en ce qui concerne les mesures de sécurité et les exigences relatives au soutien en service;

h. amélioration de la planification et du flux des travaux pour les tâches liées à la sécurité, les enquêtes ou les autres mesures correctives;

i. atténuation du risque que des processus deviennent désuets au fil de l'évolution du système d'après les données exactes concernant l'état des biens de TI;

j. augmentation de la productivité, diminution de la fatigue et réduction du stress chez le personnel technique responsable de la TI et les gestionnaires, puisqu'ils ont accès à des données plus exactes et à jour au sujet de l'état des biens de TI;

k. amélioration du moral du personnel grâce à l'augmentation de la souplesse, de l'exactitude et du rendement général du Ministère.

3 CONCORDANCE STRATÉGIQUE

3.1 Politique de défense

3.1.1 La principale responsabilité du MDN est de défendre le Canada et l'Amérique du Nord et de contribuer à la paix et à la sécurité à l'échelle internationale. Ainsi, les FAC doivent être une force militaire moderne efficace, agile, souple, bien entraînée, bien équipée et dotée des capacités fondamentales et de la souplesse requises pour répondre aux menaces conventionnelles et aux menaces asymétriques, y compris aux cyberattaques.

3.1.2 L'exercice de ces responsabilités essentielles s'appuie sur l'utilisation du cyberdomaine, qui sous-tend la capacité du MDN et des FAC à commander, à contrôler et à mener les opérations militaires. Le projet Sensibilisation à la cybersécurité améliorera la posture de cybersécurité du MDN et des FAC et diminuera le temps de réponse lors de cyberincidents.

3.1.3 Le projet Sensibilisation à la cybersécurité aidera à atténuer la menace de cyberattaques, en fournissant à l'utilisateur d'une force le moyen d'exploiter l'ITI du MDN et des FAC dans un cyberdomaine exposé aux attaques et de gérer les risques connexes. La plus grande visibilité sur le plan de la sécurité et la normalisation plus poussée qu'offrira le projet Sensibilisation à la cybersécurité établiront le fondement à partir duquel des capacités plus avancées en matière de gestion, de protection et de défense de l'ITI du MDN et des FAC, incluant notamment des mesures de défense automatisées, pourront être élaborées.

3.2 Stratégie de cybersécurité du Canada

3.2.1 La Stratégie de cybersécurité du Canada met en lumière la nécessité pour le MDN et les FAC de renforcer leur capacité à défendre leurs propres réseaux. Le projet Sensibilisation à la cybersécurité, en améliorant l'exactitude de l'information sur les réseaux et en assurant un meilleur contrôle à cet égard, permettra de s'assurer que les réseaux du MDN et des FAC demeurent protégés et défendables, ce qui contribuera à l'assurance de la qualité des missions du MDN et des FAC.

4 DESCRIPTION DÉTAILLÉE DU BESOIN OPÉRATIONNEL

4.1 Énoncé du problème ou de la possibilité

4.1.1 Les opérations militaires, quel que soit le domaine dans lequel elles sont réalisées, sont toutes liées par l'utilisation du cyberdomaine. Le cyberdomaine est un élément habilitant qui met en corrélation différents éléments (des domaines aérien, maritime, terrestre, cybernétique et spatial) afin de les amener à créer un effet orchestré, mais constitue également une source de vulnérabilité pour le MDN et les FAC, en raison de notre

dépendance aux interconnexions qu'offre le cyberespace. Les connexions au cyberespace augmentent rapidement, tant du point de vue du nombre de nœuds que de la connectivité de ces derniers (largeur de bande et fréquence de connexion). Les vulnérabilités que présente un nœud connecté au réseau peuvent être exploitées par l'adversaire pour produire des effets militaires (sabotage, espionnage ou activités d'influence) non seulement sur le nœud exploité, mais également sur d'autres appareils reliés au même réseau que ce dernier.

4.1.2 Des vulnérabilités peuvent également être introduites par un adversaire ayant entre les mains un appareil connecté au réseau. Au fur et à mesure où le nombre d'appareils et de technologies de champs de bataille en réseau augmente, il est possible qu'un de ceux-ci soit égaré accidentellement ou par la faute de l'adversaire; il serait alors essentiel de déconnecter cet appareil. Actuellement, il n'existe aucune méthode permettant de déconnecter rapidement les appareils ou de reconfigurer les paramètres de sécurité en réponse à une action militaire dynamique, dans le but de mettre fin à l'utilisation des appareils compromis.

4.1.3 Le MDN et les FAC ont besoin d'une solution technique de bout en bout, qui permettra d'accroître la sécurité des réseaux et ainsi de soutenir les cyberopérations défensives. Cette solution améliorera la confidentialité, l'intégrité et la disponibilité des données du MDN et des FAC, qui sont utilisées dans le cadre des opérations, et permettra d'apporter des modifications aux paramètres de sécurité en réponse aux opérations.

4.2 Exigences prioritaires (exigences obligatoires de haut niveau)

4.2.1 L'annexe C présente un sommaire des exigences obligatoires de haut niveau et des exigences opérationnelles préliminaires telles qu'elles sont comprises et définies à cette étape de définition du projet.

4.3 Hypothèses

4.3.1 Les hypothèses ci-dessous ont été émises dans le cadre de l'élaboration de la présente analyse de rentabilisation :

a. le MDN et les FAC dépendront de plus en plus du cyberdomaine pour mener leurs opérations, ce qui entraînera une multiplication des dispositifs non traditionnels connectés aux réseaux;

b. le cyberespace continuera d'évoluer, tout comme la nature des cybermenaces. Les menaces seront le fait d'acteurs peu qualifiés ou d'États nationaux. Le projet Sensibilisation à la cybersécurité est un des aspects de la solution de défense et de sécurité;

c. comme la cyberinfrastructure essentielle est interreliée par delà les frontières nationales, les alliés (Organisation du Traité de l'Atlantique Nord, Commandement de la défense aérospatiale de l'Amérique du Nord) exigent que les FAC sécurisent leur cyberdomaine et vice versa;

d. le code de logiciel évoluera constamment, à mesure que de nouveaux exploits seront découverts et corrigés par les fournisseurs, les alliés et les partenaires. Il faudra continuellement établir une connexion avec les appareils raccordés au réseau afin de leur distribuer ce nouveau code en vue de préserver la sécurité;

e. dans la mesure du possible, les adversaires préféreront utiliser les exploits existants, lorsque ceux-ci réussissent, sans toutefois s'y limiter.

4.4 Contraintes

4.4.1 Voici les contraintes qui ont été cernées pour le projet.

a. La solution doit respecter les architectures de référence et les exigences de sécurité du gouvernement du Canada ainsi que du MDN et des FAC;

b. la solution offerte doit permettre d'archiver des données en vue de se conformer aux politiques du gouvernement du Canada, du MDN et des FAC en matière d'archivage;

c. la solution offerte doit respecter les lois et les règlements applicables en ce qui concerne la protection et l'utilisation des renseignements confidentiels, lorsqu'il y a lieu;

d. La solution ainsi que les documents et l'instruction connexes doivent respecter la *Loi sur les langues officielles*;

e. La solution doit respecter les ententes d'échange d'information en vigueur conclues avec des alliés et d'autres ministères;

f. la solution offerte doit fournir avec souplesse des renseignements concernant l'état du réseau, qui pourront être intégrés à de futurs cyberprojets. Dépendances

4.4.2 L'on planifie actuellement des projets et des initiatives pour faire évoluer l'ITI actuelle du MDN et des FAC, ce qui influencera la mise en œuvre du projet Sensibilisation à la cybersécurité. Ces changements seront surveillés dans le cadre du projet Sensibilisation à la cybersécurité pour veiller à ce qu'il soit conforme au nouveau cyberdomaine du MDN et des FAC découlant de ces projets et initiatives. Cet aspect sera étudié plus en détail lors de l'étape de l'analyse des options et il faudra tenir compte de la future doctrine du projet Sensibilisation à la cybersécurité du MDN et des FAC.

5 PORTÉE

5.1 Limites

5.1.1 Le projet est actuellement axé sur l'offre de cyberopérations défensives améliorées dans le domaine SECRET (extensions de l'Infrastructure du réseau secret consolidé et des chefs d'état-major des armées, s'il y a lieu) et le domaine désigné déployé (Réseau étendu de la Défense). Une analyse supplémentaire sera effectuée lors de l'étape d'analyse des options pour déterminer l'application optimale du projet Sensibilisation à la cybersécurité au sein du MDN et des FAC.

5.2 Travaux compris dans le projet

5.2.1 L'objectif du projet Sensibilisation à la cybersécurité vise à accroître considérablement la capacité du MDN et des FAC de mener des cyberopérations défensives, ce qui assurera notre capacité d'appuyer les opérations militaires menées dans le cyberdomaine et par le truchement de celui-ci. Il permettra à l'organisation d'abandonner son approche d'intervention lente, manuelle et principalement réactive pour adopter une approche proactive grâce à laquelle le commandant de la mission de cyberdéfense peut anticiper et prendre des décisions rapides éclairées par renseignements et une analyse en temps quasi réel des activités sur le réseau. Cette capacité de réponse améliorée lui permettra d'exercer un commandement et un contrôle dans le cyberdomaine et d'assurer la liberté de manœuvre et la continuité des opérations. L'intégration et l'agilité du système aideront les forces de cyberdéfense à détecter les activités suspectes et elles contribueront à l'analyse des événements, au processus décisionnel et à l'intervention appropriée. Cette capacité améliorera donc la défense du cyberdomaine du MDN et des FAC.

5.2.2 Pour le moment, les travaux prévus comprennent :

a. Définition et mise en œuvre d'une suite complète comprenant les moyens techniques, le concept des opérations et la formation nécessaires pour protéger, surveiller et mettre à jour les technologies de champs de bataille en réseau et l'ITI du MDN et des FAC et en assurer la sécurité;

b. Définition et mise en œuvre d'une solution indépendante du réseau qui sera déployée sur le domaine SECRET et le domaine désigné déployé (Réseau étendu de la Défense déployé).

c. Définition et mise en œuvre d'une capacité souple intégrant l'ITI ainsi que la principale technologie de champs de bataille en réseau pour assurer l'automatisation et la tenue à jour de la sécurité.

d. Définition et mise en œuvre d'un système permettant l'intégration et l'optimisation des programmes et des projets cybernétiques des FAC servant à échanger des données.

e. Définition et mise en œuvre d'un système capable de protéger les appareils contre les menaces et les capacités actuelles. Grâce à des mises à jour, le système doit être tenu à jour et il doit protéger les appareils du MDN et des FAC contre les nouvelles menaces et capacités des adversaires dans un environnement en mutation.

f. Définition et mise en œuvre d'un système personnalisé et conçu pour le personnel du MDN et des FAC qui assure la planification, la conception, l'exploitation, la gestion, la sécurité ou la défense d'un réseau et d'une technologie de champs de bataille en réseau. Ce système est actuellement axé sur le sous-ministre adjoint (Gestion de l'information), les centres du réseau de service, la base et les unités responsables du réseau de la formation. Le programme doit être souple et modulable afin que les technologies de champs de bataille en réseau nouvelles et existantes puissent être intégrées à la connaissance du réseau qu'acquerront les communicateurs ou les techniciens de l'unité au niveau approprié;

g. Définition et mise en œuvre d'un système d'instruction que le personnel du MDN et des FAC peuvent utiliser pour veiller à ce qu'ils soient capables d'exploiter le projet Sensibilisation à la cybersécurité.

5.3 Produits livrables

5.3.1 La mise en œuvre du projet Sensibilisation à la cybersécurité comprendra du matériel, des logiciels et des processus opérationnels connexes. Les principaux produits livrables de ce projet sont les suivants :

a. mise en service de nouveaux logiciels et de nouveau matériel pour appuyer la collecte, l'analyse et l'exploitation de sources de données appropriées concernant l'état de l'ITI en matière de sécurité;

b. amélioration de processus opérationnels (y compris des indicateurs de rendement ainsi que des mesures et des systèmes de production de rapports), notamment des processus existants modifiés et des processus nouvellement définis. Ces processus opérationnels exploiteront le matériel et les logiciels pour établir une connaissance de la situation en matière de cybersécurité relativement à l'ITI, qui sera fiable, pertinente et efficace et qui touchera tous les aspects des opérations du MDN et des FAC;

c. instruction et éducation des commandants stratégiques et opérationnels (et du personnel) au sujet de leur rôle en lien avec la cybersécurité et de la façon dont l'information tirée du système découlant du projet Sensibilisation à la cybersécurité sera exploitée pour renforcer la sécurité stratégique et opérationnelle;

d. instruction du personnel technique de TI pour fournir des renseignements sur la cybersécurité stratégiques et pertinents sur le plan opérationnel aux commandants stratégiques et opérationnels (ainsi qu'au personnel);

e. une capacité de soutien en service pour maintenir et optimiser les processus opérationnels, le matériel et les logiciels ainsi que l'instruction du personnel pour veiller à ce que la capacité demeure fiable et pertinente sur le plan opérationnel pendant toute la durée de vie prévue.

6 ÉTAT DU PROJET

6.1 Généralités

6.1.1 Le projet Sensibilisation à la cybersécurité en est au début de l'étape de l'analyse des options, ce qui signifie que l'analyse de rentabilisation et la justification du projet ne sont pas achevées. Par conséquent, aucune décision n'a été prise sur les concepts, les technologies ou les approches de la solution. L'objectif de l'étape d'analyse des options est de veiller à ce que la haute direction du Ministère puisse déterminer la meilleure façon de définir le projet (c.-à-d. prendre une décision éclairée lors de l'étape de la définition) et, si elle le juge approprié, mettre en œuvre le projet pour établir la capacité requise.

6.1.2 L'on prévoit achever l'analyse de rentabilisation requise ainsi que les documents d'approbation de projet connexes d'ici septembre 2017.

6.2 Description des options

6.2.1 Lors de l'analyse de rentabilisation initiale du projet (parties 1 et 2), l'on a relevé quatre options principales qui pourraient répondre aux exigences en matière de capacité. Pour toutes les options décrites, le coût total de possession pour l'ensemble du cycle de vie de la capacité constitue la base de l'analyse de rentabilisation. Ainsi, le MDN et les FAC n'excluront aucune autre option présentée si son coût total de possession justifie un examen plus approfondi. L'objectif vise à sélectionner l'option offrant la capacité appropriée au MDN et aux FAC, et ce, de la manière la plus rapide et rentable pour le gouvernement du Canada.

a. **Option 1 — statu quo.** La sélection de cette option n'entraînera aucun changement et le MDN et les FAC continueront de protéger et de comptabiliser leurs biens d'infrastructure de réseau à l'aide des méthodes existantes. Il a été déterminé que cette option ne répond pas aux besoins opérationnels, puisque les processus existants sont manuels et que l'information ne peut pas être obtenue rapidement pour prendre des décisions efficaces en ce qui concerne les risques. Des changements sont apportés aux réseaux à un rythme qui dépasse la capacité actuelle à suivre de près la configuration. Cette option est présentée à des fins de comparaison.

b. **Option 2 – Intégration.** Selon cette approche, le MDN et les FAC tenteraient d'établir la capacité requise, en élaborant une solution à l'aide des outils actuels de surveillance en service de l'ITI et en concevant des logiciels personnalisés, au besoin. Le MDN et les FAC seraient les principaux responsables de la gestion de projet et de l'intégration et seraient appelés, à ce titre, à définir les paramètres de la capacité recherchée, à sélectionner les produits requis pour mettre en œuvre cette fonctionnalité, à intégrer et à installer les produits existants dans ce système, à les configurer et à en faire l'essai. En outre, le MDN et les FAC seraient responsables de l'exploitation et de l'entretien continus de la solution. Le personnel nécessaire à l'exécution de cette option comprendrait du personnel militaire, des fonctionnaires et des employés contractuels. Cette option suppose que l'ensemble actuel de produits de surveillance en service de l'ITI puisse être intégré avec succès en vue d'obtenir la fonctionnalité désirée et qu'un minimum de logiciels personnalisés sera nécessaire.

c. **Option 3 — achat.** L'option 3 est d'examiner la possibilité, pour le MDN et les FAC, d'acquérir une capacité complètement automatisée et intégrée en faisant appel à un intégrateur de systèmes principal. Il pourrait être nécessaire de remplacer des systèmes existants pour offrir une solution automatisée et synchronisée assurant la sensibilisation à la sécurité globale requise. Pour cette option, il pourrait être plus rentable de remplacer une partie ou même la totalité de l'ITI par une architecture et des composants à la fine pointe qui répondent à toutes les exigences obligatoires du projet. Le principal intégrateur de systèmes proposerait une solution (répondant le mieux possible aux objectifs liés au coût total de possession), il acquerrait ou créerait tous les produits nécessaires, puis mettrait en œuvre la capacité. Du point de vue du MDN et des FAC, il s'agit d'une approche « à guichet unique » offrant une capacité complète et intégrée.

d. **Option 4 – Acquisition et intégration.** Selon l'option 4, le MDN et les FAC feraient l'acquisition d'un ou de plusieurs produits disponibles sur le marché et y intégreraient, dans la mesure du possible, des composants, des systèmes et des logiciels individuels achetés précédemment afin d'établir la capacité requise. Pour mettre en œuvre cette option, le MDN et les FAC dirigeraient la gestion de projet et l'intégration afin de concevoir les paramètres de la capacité, de sélectionner les produits nécessaires à la mise en œuvre des fonctions et d'intégrer, de mettre à l'essai, d'installer et de configurer les produits existants dans ce système. Le MDN et les FAC seraient responsables de l'exploitation et de la maintenance continue de la solution. Le personnel nécessaire à l'exécution de cette option comprendrait du personnel militaire, des fonctionnaires et des employés contractuels.

7 MÉTHODE D'ANALYSE DES OPTIONS

7.1 Aperçu général

7.1.1 L'étape d'analyse des options vise à examiner et à évaluer les options générales définies, à achever l'analyse de rentabilisation, puis à recommander l'option privilégiée pour faire avancer le projet jusqu'à sa mise en œuvre. Le travail est donc axé sur l'élaboration et l'achèvement de ce qui suit :

a. L'analyse de rentabilisation (parties 1 à 5), appuyée par un EBO préliminaire élaboré en consultation avec des intervenants opérationnels et de l'industrie et les données sur les coûts générées avec l'aide de l'industrie;

b. un plan complet sur la réalisation de l'étape de définition (y compris les coûts) comprenant une stratégie intégrée d'approvisionnement en matière de défense fondée sur les faits et l'expérience tirés de la séance de mobilisation de l'industrie tenue lors de l'étape d'analyse des options;

c. un plan indicatif sur la réalisation de l'étape de mise en œuvre (y compris les coûts);

d. un plan indicatif sur l'approche de soutien en service et d'exécution des opérations après la mise en œuvre (y compris les coûts).

7.1.2 Une fois que ces travaux, les documents, les examens des jalons et les contrôles de gestion de programme nécessaires seront achevés, le projet sera présenté aux fins d'examen, d'appui et d'approbation à la Commission indépendante d'examen des acquisitions de la Défense, au Conseil des capacités de la Défense, au Conseil de gestion du programme et, finalement, au responsable investi du pouvoir délégué d'approbation de projet.

7.2 Méthode d'évaluation

7.2.1 Les critères présentés au **Error! Reference source not found.** établissent un ensemble d'exigences minimales en fonction desquelles chaque option viable sera évaluée. Ces critères d'évaluation seront fondés sur les retombées industrielles et technologiques, les propositions de valeur et toute autre modalité exigée par le gouvernement du Canada pour assurer la sécurité du contrat. Veuillez noter qu'il s'agit d'une approche d'évaluation proposée. Par conséquent, le Canada peut décider de modifier l'approche pour satisfaire aux exigences à mesure qu'elles se développent.

Tableau D 1 — Critères d'évaluation initiaux

Critère	Description
Exigences opérationnelles	L'option doit renforcer la sécurité du réseau et des technologies de champs de bataille en réseau du MDN et des FAC. L'option doit permettre de satisfaire toutes les exigences de haut niveau décrites à l'annexe C qui figurent également dans l'EOB approuvé. Il faut tenir compte des éléments suivants : a. fonctionnement général; b. rapports et alertes; c. fonctions de commande de l'exploitant; d. classification de sécurité; e. surviabilité; f. maintenance et soutien; g. disponibilité opérationnelle; h. fiabilité; i. durabilité de l'environnement; j. santé et sécurité; k. exigences d'exécution; l. besoins en matière de personnel et d'instruction; m. éléments divers.
Coût	Ce critère fait référence au coût total de possession pendant toute la durée de vie de la capacité, ce qui comprend les coûts de définition de projet, de mise en œuvre et de soutien en service à long terme. Il est essentiel que le coût total de l'option et les coûts des composants respectent l'enveloppe budgétaire (à déterminer) et que le coût total de possession soit le plus faible possible : • coûts de définition (gestion de projet [gouvernement et fournisseurs], services et matériel); • coûts de mise en œuvre (gestion de projet [gouvernement et fournisseurs], services, instruction initiale et matériel); • coûts de fonctionnement (gestion des capacités [gouvernement et fournisseurs], opérations, maintenance, instruction et exercices continus et soutien en service).
Risque	Les aspects suivants de l'option ne doivent pas présenter des niveaux de risque inacceptables : • faisabilité technique, y compris la sélection et l'instruction du personnel; • gestion de projet; • sécurité; • approvisionnement; • soutenabilité; • coût; • calendrier.

7.2.2 Lors de l'étape de l'analyse des options, le personnel responsable du projet doit déterminer la mesure dans laquelle chacune des options viables satisfait les critères suivants.

a. **Harmonisation stratégique.** Décrire en quoi l'option appuie l'architecture opérationnelle actuelle du MDN et des FAC, les résultats prévus des programmes et les résultats stratégiques décrits ci-dessus.

b. **Harmonisation avec les résultats opérationnels souhaités.** Procéder à une analyse des résultats de l'option et présenter un résumé des constatations pour chaque résultat opérationnel décrit ci-dessus.

c. **Coûts.** Fournir une description complète de tous les coûts du projet. Les estimations des coûts seront fondées sur le coût total de possession, ce qui comprend les coûts permanents engagés durant le cycle de vie de l'investissement, ainsi que les éventuels coûts de conformité pour tout groupe d'intervenants désigné.

d. **Analyse coûts-avantages.** À partir des coûts établis pour chacune des solutions, décrire comment ceux-ci sont évalués en fonction des avantages. Procédez à l'analyse coûts-avantages de chaque option en tenant compte des coûts, des avantages et des risques.

e. **Considérations relatives à la mise en œuvre et à la capacité des options viables.** Démontrer la capacité de l'organisation responsable de réaliser l'investissement et de le gérer tout au long de son cycle de vie.

f. **Passation de marchés et approvisionnement.** Fournir des renseignements concernant le mécanisme d'approvisionnement et préciser comment il sera utilisé.

g. **Calendrier et approche.** Déterminer les domaines de travail essentiels et les jalons qui leur sont associés.

h. **Incidence.** Mener une évaluation de l'incidence tant d'un point de vue interne qu'externe.

i. **Capacité.** Décrire la capacité du MDN et des FAC de gérer efficacement l'investissement si cette option est choisie.

j. **Risque.** Cerner et évaluer les risques pour chaque option, puis élaborer un plan d'action.

7.3 Justification et recommandation

7.3.1 En plus des données recueillies pendant l'étape d'analyse des options, le personnel responsable du projet doit fournir ce qui suit :

a. Résumé de la comparaison. Présenter les options viables (y compris l'option du statu quo utilisée comme point de référence) et les comparer en fonction d'un ensemble normalisé de critères (financiers et non financiers). Il serait peut-être préférable de présenter les résultats de la comparaison dans un tableau.

b. Recommandation pour l'option préconisée. Présenter la recommandation de manière directe en expliquant clairement la raison pour laquelle l'organisation profitera du fait d'investir dans une option en particulier.

c. Facteurs décisifs. Déterminer les facteurs décisifs (financiers et stratégiques) qui ont entraîné la sélection de l'option préconisée.

d. Coûts. Rédiger un résumé des estimations des coûts liés à l'option préconisée et établir des liens entre celles-ci et les composantes des domaines de travail.

e. Risques. Un exposé des faits peut être inclus pour préciser davantage le contexte entourant les principaux facteurs qui appuient l'évaluation globale des risques, par exemple, l'incidence, la probabilité et les résultats.

f. Plan pour l'étape de la définition et l'étape de la mise en œuvre. Préciser comment le projet sera défini et mis en œuvre au moyen d'un plan de travail stratégique afin de démontrer que l'investissement proposé a fait l'objet d'une réflexion approfondie et que les estimations présentées respectent un degré d'exactitude acceptable.

8 COMMENTAIRES DE L'INDUSTRIE

8.1 Présentation

8.1.1 Puisqu'une très grande partie de l'information requise pour réaliser une analyse des options approfondie et pertinente provient de l'industrie en général et que la réussite du projet dépendra totalement de la capacité de l'industrie de fournir la solution requise et d'offrir un soutien, l'industrie sera mobilisée et consultée activement tout au long des étapes d'analyse des options et de définition en vue d'élaborer une stratégie d'approvisionnement en matière de défense cohérente et efficace pour que l'état final du projet soit un succès.

8.1.2 Les commentaires de l'industrie recueillis pendant les étapes d'analyse des options et de définition aideront l'équipe de projet du MDN et des FAC à déterminer ce qui suit :

a. un EBO défini d'une manière que l'industrie peut comprendre et conforme au contexte opérationnel du MDN et des FAC, ce qui permet de mieux décrire la concordance stratégique et les besoins opérationnels du MDN et des FAC;

b. « l'art du possible » en ce qui concerne les capacités de TI de l'organisation, les nouveautés à venir dans l'industrie et la façon dont les grandes organisations semblables évoluent pour s'adapter aux changements qui touchent les exigences et les technologies en vue de mieux définir l'EBO, le budget et les échéances nécessaires pour atteindre les objectifs du projet (sur les plans technologiques, industriels et de l'approvisionnement);

c. les répercussions sur les personnes, les processus et les technologies des divers concepts proposés ainsi que les changements organisationnels qui seront nécessaires pour appuyer chaque solution conceptuelle;

d. la nature et les sources des coûts du projet, y compris la nécessité des tâches de l'étape de définition, les coûts de l'étape de mise en œuvre et le soutien en service à long terme;

e. la stratégie d'approvisionnement la plus appropriée qui peut être mise en œuvre avec l'industrie pour permettre au MDN et aux FAC d'obtenir rapidement le bon équipement et de tirer profit des achats pour créer des emplois, favoriser la croissance économique et simplifier les processus d'approvisionnement.

8.2 Réponse à la lettre d'intérêt

8.2.1 L'industrie est invitée à répondre à cette lettre d'intérêt et à fournir les renseignements suivants au plus tard à la date et à l'heure de clôture établies. L'on demande aux répondants de prendre en considération les éléments suivants lorsqu'ils préparent leur réponse.

a. Le répondant peut utiliser la mise en page de son choix. Par contre, il doit conserver la même numérotation des sections afin de faciliter l'analyse et l'examen subséquents des réponses par le gouvernement du Canada.

b. Le nombre de pages de la soumission du répondant n'est pas limité. Toutefois, la longueur du document ne devrait pas dépasser 30 pages de format lettre, imprimées d'un seul côté.

c. Les réponses doivent être soumises par écrit dans un document en format PDF. La mise en page de la soumission doit suivre le format proposé ci-dessous.

1) **Section 1 : Sommaire.** Une à deux pages résumant l'ensemble de la soumission.

2) **Section 2 : Profil de l'entreprise.**

a) Désigner la personne-ressource principale du répondant.

b) Fournir une brève introduction et une description des capacités de l'entreprise, présenter les produits, les services, les capacités en territoire canadien et l'expérience dans la prestation de solutions liées aux objectifs du projet.

c) Préciser l'intention d'être le principal intégrateur du système, un sous-traitant potentiel ou un fournisseur de produits ou de services.

d) Décrire des partenariats établis avec d'autres industries, s'il y a lieu, qui offriraient un avantage pour l'élaboration des exigences relatives aux capacités du projet.

e) Présenter toute hypothèse, contrainte, préoccupation, conclusion ou recommandation importante qui, selon le répondant, devrait être prise en considération par le gouvernement du Canada lors de l'évaluation des diverses options du projet.

3) **Section 3 : Observations et conseils.** L'on demande aux répondants de fournir des commentaires, des remarques et des conseils au sujet :

a) des questions présentées dans le document principal de la lettre d'intérêt;

b) des scénarios opérationnels décrits à l'annexe B;

c) des exigences décrites à l'annexe C;

d) de la méthode d'analyse de rentabilisation décrite à l'annexe D.

4) **Section 4 : Autres commentaires.**

a) Indiquer tout autre secteur d'intérêt qui aiderait à formuler une recommandation aux fins d'amélioration.

b) Quelles devraient être les qualifications minimales pour qu'une entreprise participe à ce projet?